Order F26-01

CITY OF RICHMOND

Michael Harvey
Information and Privacy Commissioner

January 14, 2026

CanLII Cite: 2026 BCIPC 1
Quicklaw Cite: [2026] B.C.I.P.C.D. No. 1

Summary: The City of Richmond (the City) commenced field testing a video surveillance program to collect and disclose footage to the RCMP to assist in identifying criminal suspects. The Commissioner determined that the City is not authorized to collect personal information pursuant to the program for the purpose of law enforcement (s. 26(b)), as a program or activity of the public body (s. 26(c)), or for the planning or evaluation of a program or activity of the public body (s. 26(e)). The Commissioner also concluded that the City did not provide adequate notification to individuals of the purposes and authority for collecting their personal information, contrary to s. 27(2) of FIPPA. The Commissioner required the City to stop collecting personal information through the program, delete recordings, and disband the equipment.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, ss. 26(b), (c), (e) and s. 27(2).

ISSUES

The issues to be decided in this inquiry are whether the City has the authority to collect personal information through its Public Safety Camera System (PSCS) for the purpose of law enforcement (FIPPA s. 26(b)), as a program or activity of the public body (s. 26(c)), or for the planning or evaluation of a program or activity of the public body (s. 26(e)). Further, the Commissioner also considered whether the City provided adequate notification to individuals of the purposes and authority for collecting their personal information, pursuant to s. 27(2) of FIPPA.

DISCUSSION

Beginning in February 2025, the City commenced field testing a video surveillance program called the Public Safety Camera System. The project involves the use of

multiple high-resolution intersection cameras that collect video footage of individuals, licence plates, and vehicle identification features. The sole purpose of the PSCS is for the City to collect and disclose the video footage to the Royal Canadian Mounted Police (RCMP) to assist the RCMP in identifying criminal suspects.

The field testing involves the use of cameras at the intersection of Minoru Boulevard and Granville Avenue in Richmond. The City's field testing was designed to evaluate the technical capabilities of different cameras, how many cameras to use, where to place them, and whether the PSCS could provide adequate footage for the RCMP's use.

The Office of the Information and Privacy Commissioner (OIPC) conducted an investigation pursuant to s. 42(1) of *Freedom of Information and Protection of Privacy Act* (FIPPA) into the field testing of the PSCS. The OIPC specifically considered whether the City is authorized by s. 26 of FIPPA to collect personal information pursuant to the program for the purpose of law enforcement (s. 26(b)), because it is necessary for a program or activity of the public body (s. 26(c)), or for the planning or evaluation of a program or activity of the public body (s. 26(e)). The result of that investigation was published in Investigation Report 26-01 (the Report). The Report is attached as Appendix A to this order and forms part of this Order.

As set out in the Report, the OIPC concludes that the City is not authorized by ss. 26(b), (c) or (e) of FIPPA to collect, use, and disclose personal information through the PSCS or its field test. Specifically, FIPPA does not authorize the City to collect personal information through PSCS or its field test for the purposes of law enforcement, for a City program or activity, or for planning or evaluating a City program or activity. As a result, the collection of personal information has been undertaken contrary to s. 26 of FIPPA. Further, the OIPC concludes that the City has not provided adequate notification to individuals of the purposes and authority for collecting their personal information, contrary to s. 27(2) of FIPPA.

The OIPC made the following recommendations to the City:

1. The City immediately stop collecting personal information through the PSCS.
2. The City immediately delete all PSCS recordings to date.
3. The City disband PSCS equipment used to collect personal information.

On November 12, 2025, the OIPC sent the City an embargoed copy of the Report and asked the City to respond with an indication as to whether it would comply with the three recommendations in the report. The OIPC confirmed that if the City was not willing to follow the recommendations, the Commissioner may issue an order pursuant to s. 42(1)(b) of FIPPA.

On November 24, 2025, the City responded by stating it does not intend on complying with the recommendations in the Report and expects an order to be issued.

As a result of the City's refusal to follow the recommendations in the Report, I have determined it is necessary to issue a binding order.

CONCLUSION

Pursuant to s. 42(1)(b) and 58(3)(e) and (f) of FIPPA, I make the following order:

1. The City immediately stop collecting personal information through the PSCS in contravention of s. 26 of FIPPA.
2. The City immediately delete all PSCS recordings to date.
3. The City disband PSCS equipment used to collect personal information.

I require compliance by the date of the issuance of the order. As a condition under s. 58(4) of FIPPA, I require the City to provide me with written evidence of its compliance with the above order by February 26, 2026.

January 14, 2025

ORIGINAL SIGNED BY

Michael Harvey
Information and Privacy Commissioner

OIPC File No.: F25-00259

Appendix A: OIPC Investigation Report 26-01

Office of the Information and Privacy Commissioner for British Columbia

Investigation Report 26-01

Investigation of City of Richmond's Public Safety Camera System Field Test

January 2026

CANLII CITE: 2026 BCIPC 2
QUICKLAW CITE: [2026] B.C.I.P.C.D. No. 2

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

WHO WE ARE

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including:

• The *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and

• The *Personal Information Protection Act* (PIPA), which applies to any private sector organization (including businesses, charities, non-profits, and political parties) that collects, uses, and discloses the personal information of individuals in BC. PIPA also applies to any organization operating in BC that collects, uses, or discloses personal information of any individual inside or outside of BC.

Michael Harvey is BC's Information and Privacy Commissioner.

The Office of the Information and Privacy Commissioner for BC respectfully acknowledges that its offices are located on the traditional territories of the Lekwungen people of the Songhees and Esquimalt Nations.

As an Officer of the Legislature, the work of the Commissioner spans across British Columbia, and the OIPC acknowledges the territories of First Nations around BC and is grateful to carry out our work on these lands.

CONTENTS

COMMISSIONER'S MESSAGE

Surveillance in our communities is on the increase in British Columbia. It takes many forms, including devices worn on employees, mounted at fixed locations, or in vehicles or on drones. Surveillance also takes other forms, inside and outside of private businesses and public facilities and in public places like street corners and parks. When this trend began a generation ago, the devices were videocassette cameras and footage was often low resolution and stored temporarily. Now the devices can collect more than just video, at ever increasing levels of resolution, including audio and biometric information such as faceprints, heat signatures and gait patterns. The data can be stored forever and assessed with artificial intelligence.

The trend is driven by concerns about crime and social order in our communities among public and private organizations and, indeed, by the public themselves. These concerns are legitimate and there are certain uses for which that properly implemented surveillance can be one effective tool. However, as a society, we must avoid the temptation to too easily leap to a simple approach. Surveillance, particularly of the type available today, can be corrosive to our social fabric. The lessons of the past century are that the societies that had imposed comprehensive surveillance were left with deeply damaged values. The degree of surveillance implemented in those societies pales with what today's technology offers. Yes, people of British Columbia deserve to know that someone is watching out for them, but if we do not implement these technologies in a thoughtful, careful and limited manner, we risk slipping into a society where people feel like they are always being watched.

Further, advancements in camera technology and software make it too easy and tempting for public bodies and private sector organizations to acquire and employ high definition, zoom-quality cameras with night vision, facial recognition, audio recording, automated licence plate recognition, and other such features that, when combined, go over and above what is considered reasonable collection for the context. Such features also raise the potential for scope creep, where technology installed for one purpose is later used for other purposes.

Fortunately, we have laws in British Columbia that establish the parameters for a limited and proportional surveillance. The *Freedom of Information and Protection of Privacy Act,* which governs the provincial and municipal public sectors, and which is the legal basis for this report, establishes that public bodies must only collect information as authorized by law.

In the example set out in this report, the City of Richmond (the City) is field testing a video surveillance project they have named the Public Safety Camera System. The project, currently being tested at one intersection, collects the personal information of tens of thousands of people per day via multiple high-resolution intersection cameras. The purpose of the program is to share captured images and video with police to aid in identifying criminal suspects. Throughout this report, we describe why the City is not authorized to collect personal information through the project for law enforcement, or for any other purpose under FIPPA.

In response, I recommended that the City immediately stop collecting personal information through the Public Safety Camera System and delete all recordings. I also recommended that the City disband the system equipment. Upon reviewing an embargoed copy of this report, the City advised that it did not intend to comply with

these recommendations. In response, I have issued Order F26-01.

My office and its counterparts in various jurisdictions have sounded the alarm on surveillance for decades, advising public bodies to proceed with caution, only where necessary, and while respecting privacy legislation. Beyond concerns relating to proper legal authority, there are concerns that surveillance is not as effective as often purported and can have other harms.

The deployment of video surveillance is not neutral or objective, nor is it harmless, as its use impacts individual and collective privacy in the name of safety.

Due to the plethora of concerns related to the sale, widespread availability, and potential for misuse of high-tech surveillance equipment used to identify individuals, I have also re-issued a recommendation to the BC Government. I ask that government enact legislation to explicitly regulate the sale or installation of technologies that capture biometric information. Biometric information, such as one's faceprint, is highly sensitive personal information and government should better protect individuals across BC. Without explicitly regulating biometric data collection, we leave individuals in BC subject to the unregulated market for sale and use of such equipment, and we remain behind other jurisdictions such as Quebec, who have already enacted legislation.

Other public bodies exploring options for similar high-tech video surveillance should read this report and consider whether they have the authority to collect personal information, whether such collection is necessary and proportional to the issue at hand, and whether the proposed project actually serves the public. Privacy is a core democratic value, and upholding its protection is paramount to a free and healthy society.

Michael Harvey
Information and Privacy Commissioner for British Columbia

EXECUTIVE SUMMARY

In February 2025, the City of Richmond (the City) began field testing its Public Safety Camera System (PSCS) at the intersection of Minoru Boulevard and Granville Avenue. The PSCS uses multiple ultra-high-definition video cameras installed, and once fully implemented at key locations within Richmond, would collect video footage of individuals, licence plates, and vehicle identification features. The sole purpose of the PSCS is for the City to collect and disclose the video footage to the Royal Canadian Mounted Police (RCMP) to assist it in identifying criminal suspects.

The City's field testing was designed to evaluate the technical capabilities of different cameras, how many cameras to use, where to place them, and whether the PSCS could provide adequate footage for the RCMP's use. During field testing, the City collected personal information belonging to tens of thousands of people each day. The cameras recorded continuously, and the City retained video footage for a 48-hour period, before deletion.

The City field tested eight cameras, with various built-in capabilities including Licence Plate Recognition (LPR), person/vehicle detection, infrared, audio recording, and Facial Recognition Technology (FRT). The City confirmed that it did not use any form of FRT, or built-in audio recording during field testing, however, it tested other capabilities, such as LPR and person/vehicle detection.

The OIPC investigated the City's field testing of the PSCS under s. 42(1) of FIPPA and found that the City is not authorized under FIPPA to collect, use, or disclose personal information through the PSCS or its field test.

Specifically, FIPPA does not authorize the City to collect personal information through PSCS or its field test for the purposes of law enforcement, for a City program or activity, or for planning or evaluating a City program or activity. Further, the OIPC found that the City did not provide adequate notification to individuals of the purposes and authority for collecting their personal information.

To address the issues detailed in this report, the OIPC made three recommendations to the City:

1. The City immediately stop collecting personal information through the PSCS.
2. The City immediately delete all PSCS recordings to date.
3. The City disband PSCS equipment used to collect personal information.

The City advised that it did not intend to comply with the recommendations, and the Commissioner issued Order F26-01 on this matter.

Due to the availability of sophisticated surveillance technology to those seeking it, the potential for misuse and harm, and the relative uncertainty regarding the legal limits of biometric surveillance, the OIPC has again recommended that:

4. The BC Government regulate, through legislative amendment, technologies that capture biometric information.

Regulation of technologies that capture biometric information would help to ensure appropriate guardrails are in place to avoid overstepping of the limits or the potential misuse of such tools.

Public video surveillance can be controversial, and such surveillance is only authorized in certain circumstances. While studies on effectiveness for investigating or deterring crime have demonstrated modest results in limited contexts, the negative implications for privacy, social equality, and civil liberties may be vast. Public discourse has long raised concerns about the pervasive nature of surveillance technology and how it is deployed.

As such, the OIPC encourages other public bodies considering similar surveillance programs to review this report and findings, as well as the corresponding order, for guidance before initiating such programs.

A summary of recommendations can be found on page 51.

Order F26-01 can be found at https://www.oipc.bc.ca/rulings/orders/

BACKGROUND

The Office of the Information and Privacy Commissioner for British Columbia (OIPC) monitors the extent to which public bodies protect personal information and comply with access provisions under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Privacy rights have been recognized by the Supreme Court of Canada as having quasi-constitutional status. The Canadian Charter of Rights and Freedoms further protects privacy as a fundamental right through sections 7 (the right to life, liberty and security) and 8 (protection from unreasonable search and seizure).[1] In British Columbia, FIPPA is designed to protect individuals' privacy rights, which are foundational to a flourishing democracy.

As a public body, the City of Richmond (the City) is subject to FIPPA. In recent years, the City has engaged the OIPC in discussion around replacing or adding to their current low-resolution traffic camera system with a high-definition camera system at several intersections. The City's stated sole purpose for the Public Safety Camera System (PSCS), if fully implemented, would be to use high-definition cameras to collect clear images of faces, licence plates, and vehicle identification features to share video footage and images for law enforcement purposes to assist the RCMP in identifying suspects when criminal acts occur.

In July 2024, the City submitted a Privacy Impact Assessment (PIA) to the OIPC regarding the PSCS. Upon review, the OIPC confirmed that the new high-definition cameras would collect sensitive personal information and advised the City that it did not believe FIPPA authorizes the City to collect personal information for law enforcement purposes without their own law enforcement mandate. The City disagreed with the OIPC's interpretation of FIPPA and advised that it would implement a field test of the program to assess the cameras. Further, the City requested that the OIPC issue an Order on whether the PSCS complies with FIPPA, however an Order cannot be issued in advance of the collection of personal information.[2]

The City subsequently shared with the OIPC its plan to begin a phased field test of the PSCS at several traffic intersections, starting with Minoru Boulevard and Granville Avenue and, in March 2025, provided a sample of ultra-high-definition images the City collected using the PSCS.

The OIPC determined that the images contained personal information, such as clear images of licence plates and individuals' faces which were distinguishable inside and outside of vehicles. As a result, on May 7, 2025, the OIPC notified the City that the Commissioner commenced an investigation under s. 42(1) of FIPPA.

1. Lavigne v. Canada (Office of the Commissioner of Official Languages), 2002 SCC 53 (CanLII), [2002] 2 SCR 773, <https://canlii.ca/t/51qz>, paras. 24-25.
2. Communications with the City of Richmond.

METHODOLOGY

Issues for investigation

The issues under investigation included whether the City, throughout the PSCS field test:

1. is authorized under FIPPA ss. 26 and 32 to collect and use personal information;
2. informed individuals of the purpose and authority for collecting personal information and provided contact information of an officer or employee of the public body who can answer the individual's questions about the collection, in accordance with FIPPA s. 27;
3. is authorized under FIPPA s. 33 to disclose the personal information collected via its PSCS for the field test; and
4. has met its obligations under FIPPA s. 30 to protect personal information collected through its PSCS for the field test.

Investigative methods

The OIPC sent a series of questions to the City (along with requests for related material) designed to provide a detailed understanding of the PSCS field test. The City provided the following materials for OIPC review:

- written answers pertaining to questions about the issues for investigation;
- internal and external documents used to inform City decisions on the PSCS field test;
- camera specifications, capabilities, and other details;
- additional images of footage the City collected using the PSCS; and
- notification or signage alerting the public of the presence of cameras at the field site.

The OIPC also reviewed publicly accessible information about the PSCS from the City's website, news articles, and public sentiment on the City's initiative.

APPLICATION OF FIPPA

Personal information is defined as recorded information about an identifiable individual other than contact information.[3] Under FIPPA, public bodies may only collect, use, or disclose personal information under certain circumstances listed in the Act and, in most cases, individuals must be notified of collection.

Collection and use

For collection of personal information to be authorized, at least one of the provisions listed under FIPPA s. 26 must apply to the circumstance. The City relies on the authority to collect personal information under ss. 26(b), 26(c) and 26(e):

- s. 26(b) the information is collected for the purposes of law enforcement;
- s. 26(c) the information relates directly to and is necessary for a program or activity of the public body, and for the purposes of the field test; and
- s. 26(e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body.

Public bodies may only use personal information if one of the provisions listed under s. 32 is met. The City relies on the authority to use personal information under s. 32(a) – for reasons consistent with the purpose for which the information was collected.

Notification

With few exceptions, FIPPA s. 27(2) requires public bodies to inform individuals of the purposes and authority for collecting personal information and provide contact information for someone who can answer questions about the collection. The City relies on s. 27(3)(a), where a collection notice is not required in cases where the information is "about law enforcement".

Disclosure

Public bodies may only disclose personal information if one of the provisions listed under s. 33(2) apply (and only in cases where authority existed to collect that personal information). The City anticipates disclosing information to the RCMP under ss. 33(2)(d) and (l):

> 33(2)(d) – for the purpose the information was obtained, or for a consistent purpose
> ...
> 33(2)(l) – to comply with a subpoena, warrant or court order.

3. Contact information is defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual".

Security

Public bodies must adequately protect the personal information they collect under s. 30 of FIPPA. OIPC guidance documents outline reasonable security safeguards, which include but are not limited to:

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

The City provided a summary of their security arrangements regarding access controls, activity monitoring, incident response, data encryption, and data transfer processes. The OIPC considered potential risks and the likelihood of damage or harm in the event of an incident when evaluating the City's safeguards.[4]

4. BC OIPC. October 2020. Securing personal information: A self-assessment tool for public bodies and organizations. https://www.oipc.bc.ca/documents/guidance-documents/1372.

FINDINGS & RECOMMENDATIONS

PSCS Field Test
Authority to collect and use
Duty to notify
Authority to disclose
Duty to protect

PSCS FIELD TEST

Overview

The City began recording at the intersection of Minoru Boulevard and Granville Avenue with three cameras on February 24, 2025, two additional cameras on March 6, 2025, and the three remaining cameras on April 28, April 29, and May 23, 2025, respectively. The City advised that it commenced the PSCS field test on March 17, 2025.

The City reported that it selected the Minoru and Granville intersection due to a sufficient volume of vehicle and pedestrian traffic needed for field testing. The intersection would also undergo previously planned fibre optic and higher power output upgrades required to accommodate the field test and is near Richmond City Hall, which would allow City staff to quickly inspect and adjust the cameras.

The cameras are equipped with varying capabilities including licence plate recognition, pan-tilt-roll-zoom, multi-sensor and panoramic features. Footage is intended to be captured and evaluated for quality under all weather conditions, day and night, and through different traffic patterns.

The City's stated purpose for the field test is to assess the technical capabilities of different cameras, to plan how many cameras to use and where to place them, and to ensure the PSCS can deliver high-quality and usable footage for full implementation of the program.

Information collected

The City collects the following information from vehicles and individuals during field-testing:

- licence plate numbers;
- high-definition images of vehicle occupants (drivers and passengers);
- images of pedestrians;
- Identification features on vehicles (such as company logos, vehicle makes and models, etc.); and
- geolocation data (date and time that certain vehicles, vehicle occupants and pedestrians were at certain locations).

Camera details and specifications

Initially, the City field tested eight individual cameras,[5] which included six cameras with Pan-Tilt-Zoom (PTZ), Pan-Tilt-Roll (PTR), or Pan-Tilt-Roll-Zoom (PTRZ) capabilities (four of which have 360-degree panoramic capability), two with motor vehicle licence plate recognition (LPR) capabilities, and one with 360-degree panoramic recording capability.

The City disabled one camera on May 8, 2025, after disqualifying it from PSCS field testing due to its insufficient resolution when the field of view was zoomed in on the intersection.

5. Four of the cameras were directed eastbound, three were directed westbound, and the last camera had multidirectional capability.

Beyond the PTRZ, LPR, and panoramic recording capabilities, certain cameras have additional built-in capabilities including:

- Facial Recognition Technology (FRT);
- audio recording;
- infrared capability;
- person detection; and/or
- vehicle detection.

The City confirmed it does not use image enhancing software or utilize any form of FRT technology or FRT software for the PSCS field testing. Further, the City confirmed that it does not utilize built-in audio capabilities during field testing. The City does utilize and test the LPR and person/vehicle detection capability of cameras equipped with such features.

See Table 1 for details provided about each camera the City field tested.

Table 1 - Camera Details					
Make	**Model**	**Type/ Description**	**Direction**	**General Capabilities[6]**	**Capabilities used during field testing**
Pelco	Esprit Compact PTZ	360 panoramic PTZ	Eastbound	Infrared illumination Person detection Vehicle detection	Infrared illumination Person detection Vehicle detection
Bosch	NBE-7704-ALX	Manually adjustable/ locked position	Eastbound	Audio Infrared illumination Person detection Vehicle detection	Infrared illumination Person detection Vehicle detection
Avigilon	H5 IR PTZ	360 panoramic PTZ	Westbound	FRT[7] Audio Infrared illumination Person detection Vehicle detection	Infrared illumination Person detection Vehicle detection
Axis	Q6318-LE	360 panoramic PTZ	Westbound	Infrared illumination Person detection Vehicle detection	Infrared illumination Person detection Vehicle detection
Axis	Q6100-E	360 panoramic PTRZ Multi-sensor camera module	Four-way Multidirectional	Audio	None
Axis	Q1800-LE-3	PTR LPR	Westbound	Audio Infrared LPR	Infrared LPR
Axis	Q3819-PVE	180 panoramic PTR	Eastbound	Audio Infrared	None
Genetec	SharpVG3	LPR Manually adjustable/ locked position	Eastbound	Infrared illumination LPR Vehicle detection	Infrared illumination LPR Vehicle detection

6. As provided by the City or detailed in each specific camera fact sheet.
7. When integrated with Avigilon Unity Video Software.

While the City confirmed that it does not employ any other camera function or capability during field testin, other than those listed in Table 1, the City provided data for each camera that listed more detailed specifications and additional capabilities (whether built-in or when employed with other technology), including:

- audio detection and auto directional recording;
- licence plate querying in the video management software (VMS);
- visual firearm detection and gunshot detection;
- loitering detection and recording; and
- vehicle type, colour, and plate origin identification.

To manage the cameras and recordings, the City used the VMS provided by its camera vendor (Genetec Inc.) to view, analyze, and export PSCS field test recordings or images. The VMS included an operator-focused application that provides for real-time monitoring, access control, and event management.

Camera operation and evaluation

The City reported that it does not actively monitor PSCS cameras in real time. Instead, it operates the PSCS passively, where cameras continuously record without human involvement, once the settings and view angles are configured.

The City stated that it stores video footage for 48 hours and then automatically deletes it. Once deleted, the footage cannot be recovered.

During field testing, the City adjusts camera settings, placement, and other system configurations. The City also conducts periodic reviews to monitor performance and adjust as needed. The City evaluates preferred camera models, configurations, and number of cameras required for varying intersection designs, ultimately preparing the PSCS for broader deployment.

The City intends to run the PSCS field test for six to twelve months, evaluating technical requirements and infrastructure and security throughout. For example, the City evaluates:

- image quality and usability;
- camera placement and coverage;
- law enforcement need and scope;
- access controls and data retention;
- network and storage security; and
- system reliability.

AUTHORITY TO COLLECT & USE

One of the primary purposes of FIPPA is to safeguard personal privacy rights by preventing the unauthorized collection and use of personal information by public bodies.[8]

As the Ontario Court of Appeal has recognized in Cash Converters,[9] privacy rights have quasi-constitutional status, and should only be compromised by public bodies where there is a compelling state interest for doing so:

> [29] The right to privacy of personal information is interpreted in the context of the history of privacy legislation in Canada and of the treatment of that right by the courts. The Supreme Court of Canada has characterized the federal Privacy Act, R.S.C. 1985, c. P-21 as quasi-constitutional because of the critical role that privacy plays in the preservation of a free and democratic society. In Lavigne v. Canada (Office of the Commissioner of Official Languages), 2002 SCC 53 (CanLII), [2002] 2 S.C.R. 773, Gonthier J. observed that exceptions from the rights set out in the act should be interpreted narrowly, with any doubt resolved in favour of preserving the right and with the burden of persuasion on the person asserting the exception (at paras. 30-31). In Dagg v. Canada (Minister of Finance), 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, [1997] S.C.J. No. 63, the court articulated the governing principles of privacy law including that protection of privacy is a fundamental value in modern democracies and is enshrined in ss. 7 and 8 of the Charter, and privacy rights are to be compromised only where there is a compelling state interest for doing so (at paras. 65, 66, 71) ...

Section 26 of FIPPA recognizes that to fulfill their mandates, public bodies need to collect information. However, given the importance to individuals' personal privacy, public bodies may only collect personal information in specified circumstances.

The City relies on ss. 26(b), (c) and (e) of FIPPA as bases for its authority to collect personal information pursuant to the PSCS.

The interpretation of ss. 26(b), (c) and (e) is informed in part by s. 26(a), which declares that a public body may collect personal information only if the collection is expressly authorized under an Act. This section has been interpreted restrictively: there must be an express, not an implicit, authority to collect personal information under the relevant Act for a public body to rely on s. 26(a). Broad enabling legislation will not suffice; if it did, there would be no need for these other subsections.[10]

Section 26(b): collection for the purpose of law enforcement

Section 26(b) recognizes that where law enforcement is at issue, public bodies need flexibility in the scope of their collection of personal information.[11] Section 26(b) therefore authorizes collection of personal information where the collection is for the purposes of law enforcement.

8. FIPPA, s.2.

9. Cash Converters Canada Inc. v. Oshawa (City), 2007 ONCA 502 (CanLII), <https://canlii.ca/t/1rxpx>, para. 29.

10. BC OIPC. June 2007. Order F07-10: Board of Education of School District No. 75 (Mission), paras. 29-30. https://www.oipc.bc.ca/documents/orders/885.

11. BC OIPC. March 1998. Investigation Report P98-012: Video surveillance by public bodies: a discussion, p. 15. https://www.oipc.bc.ca/documents/investigation-reports/1192.

"Law enforcement" is broadly defined, and includes policing, and any other investigations or proceedings that lead or could lead to the imposition of sanctions or a penalty.[12]

The City takes the position that the collection of personal information during the operational phase of the PSCS, and thus the collection pursuant to the field test in which it is evaluating the PSCS, is authorized by s. 26(b). This is because through the PSCS, the City collects personal information for the purposes of law enforcement, the definition of which includes "policing". Relying on Order F25-23, the City says that "policing" for the purposes of FIPPA, means "activities carried out, under authority of a statute, regarding the maintenance of public order, detection and prevention of crime, or the enforcement of law."

The City takes the position that it will clearly be collecting information "for the purposes of" policing. The purpose of the PSCS is to collect information that can be used by the RCMP to identify offenders, with a warrant.

There is a link between policing and the PSCS insofar as the City intends to collect personal information for use by the RCMP. However, an issue rests with whether the City has a law enforcement mandate that authorizes the collection of personal information for use by the RCMP.

Across the country, privacy commissioners have concluded that it is not enough for a public body to have an interest in law enforcement to rely on law enforcement as the authorization for collecting personal information. Instead, the public body must have the statutory authority to enforce laws.[13]

The Ontario Information and Privacy Commissioner's Guidelines for Video Surveillance likewise considers that it is not enough for a public body to collect information merely because the information will be used for the purpose of law enforcement; the use of that authorization is restricted to those institutions with a law enforcement mandate:[14]

> USED FOR THE PURPOSES OF LAW ENFORCEMENT
> The wording of this second condition can give rise to some confusion. Does it mean that any institution can be authorized to collect personal information so long as it is "used for the purposes of law enforcement?" Or, is it restricted in its application to those institutions with a law enforcement mandate?
>
> The IPC's position is the latter: the institution must have a clear law enforcement mandate, ideally in the form of a statutory duty. As per the definition of "law enforcement" in section 2(1) of FIPPA and MFIPPA, this could be either with respect to "policing" or "investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings." Therefore, to justify the collection of personal information under this condition, it is not enough to claim a mere interest in policing or law enforcement investigations. [Footnotes omitted]

12. FIPPA, Schedule 1, "law enforcement".

13. BC OIPC. March 2015. Investigation Report F15-01: Use of Employee Monitoring Software by the District of Saanich, p. 21. https://www.oipc.bc.ca/documents/investigation-reports/1688.

14. Information and Privacy Commissioner of Ontario. October 2015. Guidelines for the Use of Video Surveillance, pp. 5-6. https://www.ipc.on.ca/en/resources-and-decisions/guidelines-use-video-surveillance

This position has also been explicitly accepted in Nova Scotia.[15]

Further, in BC, former Commissioner Denham stated that for a public body to rely on s. 26(b), it "must have a common law or statutory law enforcement mandate."[16] It is not enough for a public body to have an interest in law enforcement.

The requirement for a public body to have a law enforcement mandate applies irrespective of whether a public body purports to collect information for policing or other forms of investigations that could lead to a penalty. The requirement for a legal mandate for collection is implicit in the structure of s. 26, which is premised on the understanding that public bodies may need to collect personal information to fulfill their legally authorized mandates. Sections 26(a), (b), (c), (e) and (h) are all concerned with ensuring that public bodies only collect personal information where there is a proper authorization for the public body to do so.

This interpretation is also consistent with FIPPA's purposes, which include "preventing the unauthorized collection, use or disclosure of personal information by public bodies".[17] Indeed, a conclusion that any public body with a mere interest in law enforcement can collect information for that purpose would effectively allow any public body with a broad mandate to engage in surveillance, regardless of whether they have a mandate to engage in policing or undertake investigations that may result in sanctions or penalties.

The City makes three arguments in support of its assertion that it has a sufficient law enforcement mandate to authorize collection of personal information during PSCS field testing:

- The RCMP has a law enforcement mandate that should be imputed to the City;
- The City has a mandate to collect information for use by the RCMP; or
- The City has an independent mandate to police citizens through the PSCS.

The RCMP's law enforcement mandate should be imputed to the City

The City argues that the RCMP's law enforcement mandate should be imputed to the City on the basis that policing by the RCMP is policing by the City. The City observes that pursuant to the *Police Act*, it is responsible for providing the municipality with a police force. It further relies on the dictionary definitions of "policing", which include controlling an area "by means of" police, "providing [an area] with" police, or keeping an area in order "by use of police". It notes that the City "polices" the municipality by ensuring that the RCMP provides policing in its geographic area, as it is required to do pursuant to the *Police Act* ss. 3, 3.1, 15 and 17. It thus says that policing performed by the RCMP amounts to policing provided by the City.

---

15. Cape Breton-Victoria Regional School Board (Re), 2017 NSOIPC 9 (CanLII), <https://canlii.ca/t/hxsgb>, para. 148.
16. BC OIPC. March 2015. Investigation Report F15-01: Use of Employee Monitoring Software by the District of Saanich, p. 21. https://www.oipc.bc.ca/documents/investigation-reports/1688.
17. FIPPA, s. 2(1)(d).

The City points to other ways that it is responsible for policing in accordance with the agreements that engage the RCMP as the municipal police service for Richmond. The City notes that a number of City employees are embedded with the RCMP and provide support services to them, which have been recognized as integral to core elements of policing. The City provides an organizational chart showing a number of RCMP positions filled by City employees, when they could be filled by RCMP officers, such as Criminal Intelligence Analysts who conduct specialized research work to assist police officers with their investigations, and one Enhanced Digital Field Technical who attends crime scenes to assist RCMP officers to manage seized property.

The City bears responsibility under the *Police Act* to "provide policing and law enforcement" in the municipality. However, it is required to do so "in accordance with [the *Police Act*]" through one of the three following options:

- establishing a municipal force;
- entering into an agreement for the RCMP to provide police services; or
- contracting with another municipality to provide those services (s. 3(2)).

The City is also required to ensure policing is provided by bearing the expenses necessary to maintain law and order, providing sufficient numbers of police,[18] and providing adequate accommodation, equipment and supplies for the operation and use of the police.[19]

Where a municipality elects to employ the provincial police force, the *Police Act* requires it do so by "entering into an agreement with the minister on behalf of the government" for policing and law enforcement to be provided by the RCMP.[20] The Municipal Police Unit Agreement (the "MPUA") then structures the respective roles of the RCMP, the Province and the municipality, as well as the resources the municipality must provide to the RCMP. The City provided the Commissioner with a copy of the MPUA between the City and the Province dated April 1, 2012.

For the reasons set out below, the City's staffing evidence, the *Police Act*, and the agreements between the City, Province and RCMP all demonstrate that, while the City is responsible for funding and providing resources to the RCMP, the RCMP's policing activities are undertaken with independence from the City. Simply put, operating a camera system that the police might use is not how a municipality provides the RCMP with resources under the *Police Act.*

The Police Act and MPUA vest policing authority in the RCMP, not the City

Under the *Police Act*, a municipality's obligations in respect of law enforcement are limited. The municipality "must" provide police services through one of the three above-mentioned options set out in s. 3(2), and not by some other means. This means that the role of a municipality is to choose from among those three options.[21]

18. *Police Act,* s. 15(1)(a).
19. *Police Act,* s. 15(1)(b).
20. *Police Act*, s. 3(2).
21. *Police Act*, s. 3.

The OIPC accepts that the City has a mandate to provide the municipality with police, however, the City cannot be said to engage in "policing" by employing the PSCS. Employing the PSCS is not the provision of police to the municipality. Again, the *Police Act* stipulates the three ways a municipality can provide a municipality with police services, and operating a surveillance camera system is not among them.

In accordance with the MPUA, where a municipality engages the RCMP's municipal police unit to act as the municipal police force in the municipality, the members of the RCMP are responsible for law enforcement in the Province:

> 3.4 Those Members who form part of the Municipal Police Unit will:
>
> a. will perform the duties of peace officers;
>
> b. will render such services as are necessary to
>
> i) preserve the peace, protect life and property, prevent crime and offences against the laws of Canada and the Province, apprehend criminals, offenders and others who may be lawfully taken into custody; and
>
> ii) execute all warrants and perform all duties and services in relation thereto that may, under the laws of Canada, the Province or the Municipality, be executed and performed by peace officers;
>
> c. may render such services as are necessary to prevent offenses against by-laws of the Municipality, after having given due consideration to other demands for enforcement services appropriate to the effective and efficient delivery of police services in the Municipality.

The *Royal Canadian Mounted Police Act*,[22] likewise confirms that every officer of the RCMP is a peace officer in every part of Canada, and "has all the powers, authority, protection and privileges that a peace officer has by law."[23] As peace officers, the members are responsible for performing all duties assigned to peace officers in connection with law enforcement:

> 18 It is the duty of members who are peace officers, subject to the orders of the Commissioner,
>
> a. to perform all duties that are assigned to peace officers in relation to the preservation of the peace, the prevention of crime and of offences against the laws of Canada and the laws in force in any province in which they may be employed, and the apprehension of criminals and offenders and others who may be lawfully taken into custody;
>
> b. to execute all warrants, and perform all duties and services in relation thereto, that may, under this Act or the laws of Canada or the laws in force in any province, be lawfully executed and performed by peace officers;
>
> c. to perform all duties that may be lawfully performed by peace officers in relation to the escort and conveyance of convicts and other persons in custody to or from any courts, places of punishment or confinement, asylums or other places; and
>
> d. to perform such other duties and functions as are prescribed by the Governor in Council or the Commissioner.

22. *Royal Canadian Mounted Police Act,* R.S.C. 1985, c. R-10.

23. *Royal Canadian Mounted Police Act,* R.S.C. 1985, c. R-10, s. 11.1(1).

The MPUA expressly vests in Canada responsibility for the internal management of the municipal police unit, including its administration, determination, and application of professional police procedures.[24]

The municipality and the Province fulfill a policy and strategic direction function in respect of the municipal police unit. The commanding officer is responsible for implementing the objectives, priorities and goals as determined by the Minister.[25] The municipality's mayor (the "CEO" under the MPUA) is permitted to set objectives for the unit that are not inconsistent with the Minister's directions.[26]

The unit's commanding officer carries out their law enforcement function under the direction of the provincial Minister.[27] The member in charge of a unit acts under the direction of the mayor, and is responsible for reporting to the mayor on the matter of law enforcement in the municipality and the implementation of the mayor's objectives, as well as informing the mayor about complaints against the unit made by members of the public.[28]

Therefore, in the OIPC's view, the structure in the *Police Act* and MPUA vest in the RCMP an authority to engage in policing and/or enforce the law independently of a municipality. Where a municipality elects to provide police services by engaging the RCMP, the MPUA is specific that responsibility for management of the force remains with Canada. The *Police Act*, the MPUA and the *RCMP Act* all specifically vest in the police, not the municipality, responsibility for law enforcement and policing. It is the members of the RCMP or the municipal police department that are specifically charged with enforcing the laws of the province, preventing crime, and apprehending criminals and offenders. Those responsibilities are not vested in the municipality.

The Police Act and MPUA structure the City's obligation to resource the RCMP

A municipality is responsible for financing and providing resources for a police unit. Again, however, the City is limited in how it does so. The City must provide resources "in accordance with this Act, the regulations and the director's standards".[29] Where a municipality elects to provide policing by engaging the RCMP, the *Police Act* confirms the resources are provided by the municipality's payment to the Province of the amount the Province is liable to pay to Canada for the use of the services of the RCMP in that municipality.[30]

With respect to resourcing the RCMP, under the MPUA, the municipality is required to provide and maintain at no cost to Canada or the Province accommodation fit for use by the unit, including office space, jail facilities and garage space. It is also responsible for paying

24. MPUA, s. 4.1.
25. MPUA, s. 5.2.
26. MPUA, s. 5.3.
27. MPUA, s. 5.1.
28. MPUA, ss. 5.4, 5.5.
29. *Police Act*, s. 15.
30. *Police Act,* s. 16.

100% of all operating and maintenance costs for those resources.[31] The MPUA also confirms the municipality's obligation to pay the costs of providing and maintaining the unit in the municipality.[32]

Thus, while a municipality provides resources to the RCMP, it does so in the manner contemplated in the MPUA: through the payment to Canada a cost-sharing ratio with respect to maintenance of the municipal police unit, including contributions toward specific costs incurred by the RCMP at the national level.[33]

The OIPC accepts that the City also engages some staff who do work for the RCMP. However, it appears that although those employees are City employees, they are fully embedded in and operate at the direction of the RCMP, not the City, in the performance of their duties.

There is nothing in the MPUA that envisions the City providing the RCMP with video footage to assist it with identifying offenders such that the City could be said to be exercising a policing mandate through the PSCS.[34] At most, the City is required to compensate Canada for costs of equipment purchased by Canada.[35]

The independence of the police weighs against imputing law enforcement obligations to the City

The OIPC's view that the RCMP fulfills its policing and law enforcement mandate independently of the City is consistent with the longstanding principle that police forces must be ensured independence from the government that appoints them to protect the rule of law. As the Supreme Court of Canada recognized more than 100 years ago, police officers must never be regarded as agents or officers of a municipality. They exercise a public function and do so independently of the municipalities that appoint them.[36]

More recently, the Court has observed that police officers are public officers, and in fulfilling their law enforcement functions must be seen as independent of the executive branch of government, and not subject to political direction, to ensure the rule of law:[37]

> 33 While for certain purposes the Commissioner of the RCMP reports to the Solicitor General, the Commissioner is not to be considered a servant or agent of the government while engaged in a criminal investigation. The Commissioner is not subject to political direction. Like every other police officer similarly engaged, he is answerable to the law and, no doubt, to his conscience. As Lord Denning put it in relation to the Commissioner of Police in R. v. Metropolitan Police Comr., Ex parte Blackburn, [1968] 1 All E.R. 763 (C.A.), at p. 769:

31. MPUA, s. 10.1.
32. MPUA, s. 11.1.
33. MPUA, s. 11.
34. Recognizing that FIPPA, s. 33(2)(l) authorizes disclosure to comply with a subpoena, warrant or court order.
35. MPUA, s. 11.2(b).
36. McCleave v. City of Moncton, 1902 CanLII 73 (SCC), 32 SCR 106, <https://canlii.ca/t/ggxjg>, pp. 108-10.
37. R. v. Campbell, 1999 CanLII 676 (SCC), [1999] 1 SCR 565, <https://canlii.ca/t/1fqp4>, para. 33.

> I have no hesitation, however, in holding that, like every constable in the land, he [the Commissioner of Police] should be, and is, independent of the executive. He is not subject to the orders of the Secretary of State, save that under the Police Act 1964 the Secretary of State can call on him to give a report, or to retire in the interests of efficiency. I hold it to be the duty of the Commissioner of Police, as it is of every chief constable, to enforce the law of the land. He must take steps so to post his men that crimes may be detected; and that honest citizens may go about their affairs in peace. He must decide whether or not suspected persons are to be prosecuted; and, if need be, bring the prosecution or see that it is brought; but in all these things he is not the servant of anyone, save of the law itself. No Minister of the Crown can tell him that he must, or must not, keep observation on this place or that; or that he must, or must not, prosecute this man or that one. Nor can any police authority tell him so. The responsibility for law enforcement lies on him. He is answerable to the law and to the law alone. [Emphasis in original.]

Courts in BC and Alberta have both found that the structures of the Police Acts in those provinces were intended to give effect to this principle. In McAllister v. Calgary (City),[38] the Court explained that a legislative structure that separates governance of a police force from the municipality ensures that those tasked with law enforcement are not improperly influenced by government actors:

> [27] The policy behind this structure is sound, and is concisely set out in the following excerpt from Paul Ceyssens, Legal Aspects of Policing, loose-leaf (Update 15 - September 2002), (Earlscourt Legal Press, Inc., 1994) at p 4-13:
>
> Various justifications exist for inserting a police board between the municipal council and the police force. The most prominent reason relates to insulating the police from direct control from municipal politicians. In Bruton v Regina City Policemen's Ass'n Loc. 155, [1945] 3 DLR 437 (Sask CA), the Chief Justice of Saskatchewan offered the following analysis:
>
> In providing such a body to administer the police force, I am of the opinion that it was the intention of the Legislature to ensure a just and impartial carrying out of the duties which devolve upon constables and peace officers and to place the chief of police, the officers and the constables of the force in a position where they are removed from the influence of persons who may attempt to interfere with the due performance of police duties such as the detention and arrest of offenders, the preservation of the peace, the enforcement of laws, and other similar duties with which police officers are entrusted by law.

Henry v. British Columbia[39] adopted the reasoning in McAllister and found that BC's *Police Act* demonstrates the same legislative intent.

38. McAllister v. Calgary (City), 2012 ABCA 346 (CanLII), <https://canlii.ca/t/fttgr>.
39. Henry v. British Columbia, 2014 BCSC 1018 (CanLII), <https://canlii.ca/t/g7c7b>, para. 33.

In the OIPC's view, the intention of the legislature is clear: police have the general responsibility for law enforcement in the province. The *Police Act* is intended to ensure the independence of the police from municipalities. Imputing law enforcement or policing by the RCMP to the city would blur the lines between the municipality and the RCMP, and risk compromising the independence of the RCMP in the performance of its public function. The RCMP unit in Richmond must be seen as being completely independent of influence by the City in the investigation and enforcement of crime. A conclusion that the RCMP's law enforcement is the City's law enforcement is inconsistent with this principle.

Parenthetically, it is worth noting that there is a serious question whether the RCMP could themselves engage in the type of surveillance contemplated by the PSCS. Section 8 of the Canadian Charter of Rights and Freedoms protects against unreasonable search and seizure. That section has been interpreted as preventing surreptitious surveillance by an agency of the state for law enforcement purposes without judicial authorization. The Supreme Court of Canada has cautioned that despite the utility of electronic surveillance in the investigation of crimes, "it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion."[40]

The OIPC acknowledges that it may not be an unreasonable invasion of personal privacy for the police to employ limited video surveillance without judicial authorization as a deterrent in the context of a particular law enforcement need.[41] That said, there is good reason to question whether it would constitute an unreasonable search for the police to engage in continuously recorded surveillance with the intention that it be used for evidence gathering purposes, even if the further access to recorded material is only accessible with further judicial authorization. Of course, the question of whether surveillance of this type is contrary to s. 8 of the Charter is an issue for the courts and beyond the scope of this report.

Mandate to collect information for use by the RCMP

Alternatively, the City takes the position that it has a law enforcement mandate to collect personal information to be used by the RCMP in the RCMP's policing efforts.

The City argues that for s. 26(b) to apply, all that is required is that the collection be "for the purpose of" law enforcement. It says that is clearly the case with respect to the PSCS, which has as its sole purpose assisting the RCMP to identify suspects when criminal acts occur in the City.

The City takes the position that there is no requirement for the "policing" or "law enforcement" at issue to be undertaken by the City itself for it to be authorized to collect the information at issue; meaning, the policing or law enforcement can be undertaken by a separate law enforcement entity. The City points to the language used in ss. 26(c) and (e), which specifically require that the collection be necessary to a program or activity of "the" or "a" public body, respectively. It observes that there is no similar requirement in s. 26(b) that collection be for the purposes of law enforcement being undertaken by the/a public body.

40. R. v. Duarte, 1990 CanLII 150 (SCC), [1990] 1 SCR 30, <https://canlii.ca/t/1fszz>.

41. Papenbrock-Ryan v. Vancouver (City), 2024 BCSC 2288 (CanLII), <https://canlii.ca/t/k8fpv>, paras. 14-18.

Again, for the City's collection of personal information on behalf of the RCMP to be authorized by s. 26(b), doing so must fall within its law enforcement mandate. Notably, in analogous circumstances to this one, the Information and Privacy Commissioner of Ontario explicitly rejected an argument that collection of personal information by a municipality that was in turn disclosed to and used by a police force was authorized for the purpose of law enforcement.

The police in that case argued that they had the authority to prevent crime and enforce laws pursuant to the Ontario *Police Services Act*. The police took the position that a municipality's collection of personal information that was used by the police was authorized on the basis that it was collected for the purpose of law enforcement. The Ontario Commissioner rejected that argument on the basis that the city itself had no mandate under the *Police Services Act*, with the result that the statute did not apply to bring the collection within the law enforcement authorization.[42]

The same is true here. As set out above, the RCMP has the mandate to investigate crime. It does so independently of the City, which has no mandate under the *Police Act* or the MPUA to prevent crime or enforce the criminal law.

The City says that s. 8(2) of the *Community Charter* gives it such a mandate. That section provides:

> (2) A municipality may provide any service that the council considers necessary or desirable, and may do this directly or through another public authority or another person or organization.

Sections 8(3) through to (6) set out the areas in which a municipal council may regulate, prohibit, and/or impose requirements through bylaw. Section 10(a) in turn confirms that a municipality's powers in s. 8 "are subject to any specific conditions and restrictions established under this or another Act".[43]

The City takes the position that to have the authority to implement the PSCS it only needs to demonstrate that it has some authority to undertake a program, not that it has a law enforcement mandate. It says that it has such an authority in s. 8(2), which authorizes it to offer services. In this case, it says that it is providing a service: a service to the RCMP assisting it to identify offenders.

In OIPC's investigation report F15-01 on the *Use of Employee Monitoring Software by the District of Saanich*,[44] Commissioner Denham rejected an argument that s. 8 grants municipalities a law enforcement mandate with respect to criminal matters. That case

42. Ottawa Police Service (Re), 2007 CanLII 87532 (ON IPC), <https://canlii.ca/t/gvnpm>, p. 9.

43. *Community Charter*, s. 8(10)(a).

44. BC OIPC. March 2015. Investigation Report F15-01: *Use of Employee Monitoring Software by the District of Saanich*. https://www.oipc.bc.ca/documents/investigation-reports/1688.

concerned a municipal government using IT programs to monitor employee activity on workplace computers. The municipality argued it had the authority to do so pursuant to its law enforcement mandate, as it was monitoring illegal or unauthorized access to its computer networks.

Commissioner Denham considered that a municipality's law enforcement mandate pursuant to s. 8 is limited to the subjects enumerated in s. 8(3), including such things as regulating municipal services. It did not extend to the regulation of illegal or unauthorized access to computer networks, which was more appropriately within the jurisdiction of law enforcement agencies charged with the enforcement of the Criminal Code of Canada, such as a municipal police department. She found that a municipality could not claim a law enforcement purpose for the collection of personal information by the IT program because it had no statutory or common law mandate to enforce the Criminal Code of Canada.

The City suggests that in that case, the District of Saanich attempted to justify its collection of personal information as a regulatory effort, and therefore the OIPC report should be read as being limited to circumstances where a district is relying on its regulatory authority. The OIPC does not agree with the City's view that this case was about collection for regulatory purposes. Instead, the District collected information about employees' use of computer networks through an IT program, and there is nothing in the Investigation Report to suggest that the District was doing so pursuant to its regulatory authority in s. 8(3).

As noted in Commissioner Denham's analysis, s. 8 affords municipalities a law enforcement mandate with respect to matters within their jurisdiction. However, the broadly framed authority in s. 8(2) to provide municipal services does not go so far as to give municipalities a mandate to collect information on behalf of the RCMP. Identifying criminals is the work of a police service, not a municipality.

Further, the City's authority to offer services is subject to any requirements set out in the *Community Charter* and other legislation.[45] The means by which the City "provides policing" is subject to a detailed structure in the *Police Act* and the MPUA. The *Police Act* specifies that the City is required to provide policing and law enforcement through the means contemplated in that legislation.[46] The City does so by entering into a contract for the RCMP to police the municipality. The City is also responsible for bearing the expenses necessary to maintain law and order, and providing sufficient numbers of police,[47] and adequate accommodation, equipment and supplies for the operation and use of the police.[48] It does so by paying for services pursuant to the MPUA.

In the OIPC's view, s. 8(2) does not go so far as to afford the City an authority to provide an additional service to the police, not envisioned in the *Police Act* and the MPUA. Doing so is arguably inconsistent with the structure of the *Police Act.*

45. *Community Charter*, s. 8(10)(a).
46. *Police Act*, s. 3(2).
47. *Police Act*, s. 15(1)(a).
48. *Police Act*, s. 15(1)(b).

The City's own mandate to police the municipality

In the final alternative, the City takes the position that the PSCS is authorized by s. 26(b) because the City is engaging in policing itself through the deployment of high-definition intersection cameras that will control crime by identifying offenders. The RCMP can then use some of the collected information for further law enforcement efforts. The City says it has a mandate to do so pursuant to s. 8 of the *Community Charter,* which affords the City a broad discretion to provide whatsoever services it considers to be appropriate.

For the reasons set out above, in the OIPC's view, s. 8 does not provide the City with a law enforcement mandate with respect to criminal matters. The structure of the *Police Act* is such that policing must be provided independently of a municipality to ensure the rule of law. The RCMP, not the City, polices the municipality. While the data collected through the PSCS might be used in policing undertaken by the RCMP, the program itself is not policing undertaken by the City.

Section 26(c): collection for an authorized program or activity of the public body

Section 26(c) provides an avenue for public bodies to collect personal information that is necessary for an otherwise-authorized program or activity of the public body. As former Commissioner Loukidelis has acknowledged, legislation typically does not authorize the collection of specific types of personal information. Most statutes simply authorize programs or activities.[49] Section 26(c) recognizes that an authorized program or activity may in turn require the collection of personal information. Where a public body can show that collection is necessary to that otherwise-authorized program or activity, the collection will be authorized pursuant to s. 26(c).

To rely on this authorization, a public body must show two things:

- that the information relates directly to an authorized program or activity; and
- that the collection is necessary for that program or activity.[50]

The City's authorized program or activity

The first step is to define the program or activity that the City is engaged in to determine whether that program or activity is an authorized one, and whether the collection of information relates directly to it. Previous orders have interpreted a "program" for the purposes of this section as being "an operational or administrative program that involves the delivery

49. BC OIPC. June 2007. Order F07-10: Board of Education of School District No. 75 (Mission), para. 29. https://www.oipc.bc.ca/documents/orders/885.
50. BC OIPC. March 2015. Investigation Report F15-01: *Use of Employee Monitoring Software by the District of Saanich,* p. 21. https://www.oipc.bc.ca/documents/investigation-reports/1688.

of services under a specific statutory or other authority", or a "designed delivery of services to more than one individual"; it does not include a plan that only applies to a specific individual.[51]

The City defines its program or activity as "an intersection camera program for the identification of criminal suspects following criminal incidents in the City." It says that the installation, maintenance and operation of the cameras for that purpose is an activity undertaken or provided by the City and is thus authorized by s. 8(2) of the *Community Charter.* Of course, the actual identification of criminals will be undertaken by the RCMP, not the City.

This service on its face appears to fall within s. 8(2) of the *Community Charter* as being a service that the City considers to be necessary or advisable. However, as set out above, providing such a service cannot be reconciled with the structure of the *Police Act*, which sets out how the City is required to provide policing services and ensure that the RCMP is properly resourced. Collecting evidence to identify criminals that the RCMP may rely on does not form part of that arrangement. For the reasons already given, it is not a program or activity authorized by s. 8(2).

The necessity of the collection of personal information

The OIPC does not accept that the PSCS is an authorized program. Nevertheless, to provide guidance to other public bodies, the OIPC will consider whether the collection is necessary for the program or activity relied on by the City: an intersection camera program for the identification of criminal suspects following criminal incidents in the City.

In Order F07-10, former Commissioner Loukidelis considered the meaning of "necessary" for the purpose of s. 26(c). He concluded that it is not enough that the personal information would be nice to have or merely convenient to have, or that it could perhaps be of some use some time in the future. At the same time, "necessary" in s. 26(c) does not mean the information must be indispensable, or that it would be impossible to operate a program or carry on an activity without the personal information.[52] More recently in Order F25-01, Adjudicator Siew engaged in a statutory interpretation of the word "necessity" for the purpose of s. 34(b) of FIPPA. She likewise found that the word "necessary" means more than merely helpful but did not rise to the standard of "essential" or "indispensable".[53]

When determining whether collection is necessary for a program or activity of the public body under s. 26(c), the assessment is conducted in a searching and rigorous way, considering:

- the sensitivity of the personal information;
- the particular purpose for the collection;
- the amount of personal information collected; and
- "FIPPA's privacy protection objective" which is "consistent with the internationally recognized principle of limited collection".[54]

51. BC OIPC. October 2019. Order F19-37: Ministry of Finance, paras. 27-28. https://www.oipc.bc.ca/documents/orders/2214.
52. BC OIPC. June 2007. Order F07-10: Board of Education of School District No. 75 (Mission), paras. 48-49. https://www.oipc.bc.ca/documents/orders/885.
53. BC OIPC. January 2025. Order F25-01: Cultus Lake Park Board, paras. 82-94. https://www.oipc.bc.ca/documents/orders/2903.
54. BC OIPC. June 2007. Order F07-10: Board of Education of School District No. 75 (Mission), para. 49. https://www.oipc.bc.ca/documents/orders/885.

When undertaking the analysis, the OIPC also takes some guidance from the approach undertaken in Ontario. Following Cash Converters, the Court explained that the proper approach to determining necessity is to examine in detail the types of information being collected, and to determine whether each type is necessary for the collecting body's activity. To be authorized, the public body must show that the collection is necessary to administer the authorized activity. It is not enough for the collection to be merely helpful to the activity.

Guidance with respect to how the necessity analysis may be applied in the specific context of video surveillance by a municipality can be found in Cambridge (City) (Re), a decision of the Information and Privacy Commissioner of Ontario. That case concerned a municipality that implemented video surveillance to ensure safety of public works. The Ontario Commissioner pointed to a number of factors that are relevant to the consideration of whether video surveillance is necessary to the operation of the authorized program or service. Public bodies must consider whether:

> [33] …
> • the problem to be addressed by video surveillance is real, substantial and pressing;
> • other less intrusive means of achieving the same goals have been considered and are substantially less effective than video surveillance or are not feasible; and
> • the benefits of video surveillance substantially outweigh the reduction of privacy inherent in its use.[55]

The delegate also emphasized the need to consider the sensitivity of personal information, including the nature of the space under observation and the "closeness" of the surveillance. Public bodies should also apply the principle of data minimization: limiting the amount of information collected to that which is necessary to fulfill the purposes of the lawfully authorized activity.[56]

The City argues that it is "necessary" to collect personal information as without it, the PSCS would be completely ineffective:

> The collection of personal information is of course directly related to the City's proposed program as the collection of the personal information is an integral part of it. It is "necessary" to collect personal information, or the PSCS would not work at all. The whole purpose of the program is to use high-definition cameras to collect clear, images of license plates, faces and other identification features on vehicles (company logos, vehicle makes and models etc.) so that criminal suspects may be identified. Without the collection of personal information contemplated during the operational phase of the PSCS, none of that would be possible.[57]

The City's initial submission on s. 26(c) included no analysis of whether other, less intrusive means of identifying criminals had been considered and found to be substantially less effective than video surveillance. It likewise provided no analysis of how the benefits of video

55. Cambridge (City) (Re), 2021 CanLII 37668 (ON IPC), <https://canlii.ca/t/jfrxh>, para. 33.
56. Cambridge (City) (Re), 2021 CanLII 37668 (ON IPC), <https://canlii.ca/t/jfrxh>, paras. 40-41.
57. City's Response, June 13, 2025, p. 20.

surveillance substantially outweigh the reduction of privacy inherent in its use.

In response to additional questions from the Commissioner, the City provided more information about the issue that the PSCS is designed to address. The City confirmed that the PSCS is designed to assist in the identification of suspects in a wide array of criminal activities, including organized crime, violent crime and serious property crime. It explained that the PSCS has the potential to record offences, and individuals or vehicles involved in the course of criminal activity. It pointed to 28 specific types of crimes where it envisioned the PSCS could provide relevant evidence to assist with investigations.

The City also provided additional information about what other, less intrusive means of identifying suspects the City had contemplated. The City pointed to criminal suspect identification measures employed by the RCMP (and, it says, the City), including "the execution of search warrants, interviews with witnesses, forensic work and so on." The City indicated that the PSCS was necessary because these tactics did not result in a sufficiently high level of criminal identification. The City confirmed there was no other criminal-identification opportunity of which it was aware that would make the PSCS completely redundant or unnecessary, particularly given the City's existing CCTV system had low fidelity images making it unusable for identification purposes.

The City indicated that it had weighed the benefits of the PSCS against the reduction of privacy. It confirmed that the "political judgment was made by Council that the privacy impacts of the PSCS are not so severe as to outweigh the expected law enforcement benefits". In this connection, the City stressed that the PSCS would include no active monitoring, would restrict access to staff, and would incorporate other data safety measures, as well as disclosure to law enforcement only based on production and/or court orders.

When evaluating whether the collection of personal information through the PSCS is necessary to an authorized program or activity, it is important to bear in mind the particular risks associated with video surveillance in public spaces. More than 25 years ago, Former Commissioner Flaherty pointed to risks associated with mass video surveillance of the type envisioned by the PSCS as a result of indiscriminate recording:[58]

> While most people have an instinctive aversion to being watched, the "chilling effect" of video surveillance on public behaviour is difficult to determine. One thing is clear: issues raised by the video surveillance debate go far beyond arguments of its crime-fighting efficacy. Video surveillance in public places is as much a civil liberties issue as it is a privacy issue, and those civil liberties concerns are closely related to other prized community values, including freedom of assembly and movement.
>
> Nigel Waters points out that video surveillance, unlike more traditional forms of surveillance, is random and indiscriminate in its gaze. Video surveillance involves the collection of personal information without the consent of those under surveillance:

58. BC OIPC. March 1998. Investigation Report P98-012: *Video surveillance by public bodies: a discussion,* p. 7. https://www.oipc.bc.ca/documents/investigation-reports/1192.

> Everyone coming into view -- shoppers, children, lovers, and the socially disadvantaged -- is captured by the cameras recording the movements of daily life without regard to whether a crime is being or is likely to be committed and with no grounds for suspicion because most cameras cannot be made simply to record particular incidents or serious crimes. Everyone suffers the infringement of their privacy and of the right to go about their daily lives free from surveillance.
>
> [Footnotes omitted.]

In Cambridge (City) (Re), the delegate of the Information and Privacy Commissioner of Ontario pointed to a similar concern in connection with the proposed municipal camera system:

> [53] However, in determining whether the collection of personal information by a video surveillance system is "necessary", I note the Guidelines explanation of the risks of video surveillance to privacy as follows:
>
> While video surveillance may help to increase the safety of individuals and the security of assets, it also introduces risks to the privacy of individuals whose personal information may be collected, used and disclosed as a result of the technology. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be taken when considering whether and how to use this technology.

The collection of personal information by the PSCS field test involves pervasive, continuous collection of personal information. The City captures footage and images of identifiable faces, licence plates, and car makes and models. It collects information about pedestrians and motorists going about their daily lives. While the information may not be continuously monitored and may be held for only a short period of time, the collection of personal information is significant. Most of the personal information collected will have no relationship at all to the detection of criminals.

The City suggests that the collection is nonetheless warranted because existing policing measures are not sufficiently effective, and some crimes are going unresolved. The City provided some evidence of the types of crimes that the collected information might help to resolve. That said, the evidence falls short of establishing that existing policing measures are ineffective, or that the issue of unresolved crime in Richmond is real, substantial, and pressing. Further, evidence the City provided of other less intrusive means it had considered was limited. It appears the City only considered its existing CCTV system, the PSCS, and current policing methods.

Put simply, the City put forward a limited record to demonstrate that the PSCS would assist with the identification of criminals, or that alternative means, including routine policing, were ineffective. However, it is clear that the intrusion into the citizens' privacy would be vast.

The OIPC finds that the PSCS is not an authorized program of the City. Even if it were, the OIPC is not satisfied that the City has established that the collection of personal information by the PSCS is necessary to the City's stated program or activity.

Section 26(e): planning and evaluating a program or activity of the public body

The City also relies on s. 26(e), which authorizes collection where the information is necessary for the purposes of planning or evaluating a program or activity of a public body. The City appears to accept that s. 26(e) is operative only where a program or activity being planned or evaluated is one a public body is authorized to undertake. It also accepts that the collection must be "necessary" for the purpose of planning or evaluating the program or activity at issue. It allows that necessity is a rigorous standard, that goes beyond mere convenience but does not require that the program or activity be impossible to carry out without it.

The City says that collection in the field test is necessary to evaluate the PSCS. It notes that the field test aims to verify that the technical requirements are met, ensure the cameras will reliably capture information, determine acceptable standards for the video images for law enforcement purposes, identify blind areas, determine the required number, make, model and configuration of cameras, assess the performance of the cameras across weather and lighting conditions, and assess camera durability. The City is also making efforts to ensure that collected images are viewed by limited personnel and protected from unauthorized disclosure.

The City's reliance on s. 26(e) is contingent on the City's collection being authorized by ss. 26(b) or (c). The OIPC agrees – the City will only be able to rely on s. 26(e) if the PSCS is otherwise authorized. Given the findings above that the PSCS is not authorized by ss. 26(b) or (c), the City is unable to rely on s. 26(e).

As such, the OIPC recommends that the City immediately stop collecting personal information through the PSCS field test, delete all remaining recordings, and disband the cameras and other equipment used to collect personal information for the PSCS field test.

Recommendation 1

The City should immediately stop collecting personal information through the PSCS.

Recommendation 2

The City should immediately delete all PSCS recordings to date.

Recommendation 3

The City should disband PSCS equipment used to collect personal information.

Upon reviewing an embargoed copy of this report, the City advised that it did not intend to comply with these recommendations. Subsequently, the Commissioner issued Order F26-01[59] on this matter.

59. https://www.oipc.bc.ca/rulings/orders/

DUTY TO NOTIFY

Requirement to notify individuals

The City relies on s. 27(3)(a) as an authority relieving it from the requirement to provide notice pursuant to s. 27(2) of FIPPA. The City argues that all of the information it is collecting during the testing phase concerns or relates to the City's law enforcement objective and is therefore "about" law enforcement because it is information that is necessarily collected to achieve a law enforcement objective and for no other purpose.

For all the reasons given above, the City is not entitled to rely on law enforcement as an authorization to implement the PSCS. This is sufficient on its own to dispose of the City's argument.

Moreover, at the testing phase, law enforcement is not the focus of the collection. The City confirmed in its submission that the field test is not being used for actual public safety purposes. The OIPC asked the City whether information collected during the field test would be used to monitor public events, riots, protests, internal investigations, and so on. The City confirmed that it intended to make no use of the information other than testing the cameras:

> The City will not be collecting or using personal information during the field testing phase for any purpose other than planning and evaluating the City's proposed PSCS. It will not be collecting or using personal information in any of the manners identified in the examples. The field test is very narrowly constructed to allow only such collection and use as is necessary to properly plan the program so as to achieve the objects of the operational phase of it – the identification and subsequent prosecution of offenders. The City has not contemplated, as regards the operational phase of the program, any collection or use of personal information beyond that which is identified in the PIA.[60]

In those circumstances, it is arguable that even taking into account the broad interpretation of "about law enforcement" in s. 27(3)(a), the collection of personal information at the testing phase is not being undertaken for the purpose of law enforcement. The information will not be used to enforce any laws. It will be used to evaluate the technical capabilities of the cameras. In those circumstances, there is no compelling law enforcement purpose that weighs against providing notice to the public.

As the City cannot rely on s. 27(3)(a) FIPPA to relieve it from notifying individuals it collects personal information from during field testing, the OIPC next examined whether the City notified individuals in accordance with s. 27(2) FIPPA.

Inadequate notification

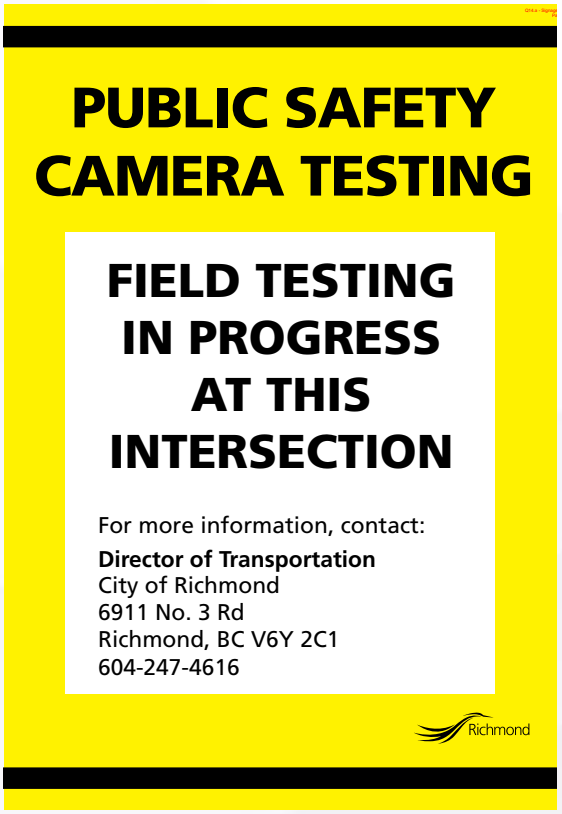
The City indicated that it installed the following signage on February 13, 2025, as a courtesy

60. City's Response, June 13, 2025, p. 21.

and for transparency purposes (rather than to fulfill a legal obligation).

The City installed this signage adjacent to the:

- Eastbound driving lanes of Granville Avenue, approximately 53 metres before the intersection; and
- Westbound driving lanes of Granville Avenue, approximately 76 metres before the intersection.



The City stated that PSCS signage is vehicle-focused, oriented in the direction of vehicle travel, and placed to ensure it was clearly visible and legible in advance of the intersection to allow drivers time to read the signs. The City advised that it did not plan to install PSCS signage at the intersection targeted towards pedestrians or place signage at any other location where vehicles, pedestrians, or others may enter the intersection or be captured by the PSCS.

The OIPC has concerns about the content and location of the signage.

First, the content of the signage is vague and ambiguous as it does not notify individuals that cameras are recording and collecting personal information and does not include the purposes or authority for collection, as required by FIPPA s. 27(2). Stating simply that field testing is in progress does not meet the legislated requirements.

Second, the placement of the signs does not consider individuals in vehicles who may enter the intersection from the north or south, nor does it notify pedestrians entering the intersection from any direction, despite the ability of many of the cameras to pan 360 degrees and one camera (Axis Q6318-LE) to record simultaneously in multiple directions.

Considering the deficiencies in the both the content and placement of the signs, the City did not adequately notify individuals when it collected personal information from individuals during field testing.

The City advised that it would be willing to review existing signage and make any changes needed to ensure compliance with s. 27(2) FIPPA. However, as the City is not authorized to collect personal information through the PSCS and the OIPC has recommended that the City disband the PSCS, there is no recommendation for the City to amend its notification.

AUTHORITY TO DISCLOSE

Although no disclosure has occurred at the time of this report, the City confirmed that it anticipated disclosing personal information during the field test under limited circumstances under ss. 33(2)(d) and (l).

Section 33(2)(d)

The City stated that personal information would be disclosed in a limited way with the RCMP under s. 33(2)(d) for the purposes of evaluating the cameras and quality of the footage, which authorizes disclosure if there is a consistent purpose for which it had been collected. The City confirmed that the RCMP would be provided with access to randomized recorded footage, as well as randomized live footage under City staff supervision at a later phase of the field test. Although the City has yet to disclose personal information to the RCMP for the purposes of the field test, the City estimates this review process would take between one-to-two months once it begins. Any disclosure in this phase would only be for evaluating the cameras and not for law enforcement purposes.

As discussed above, the OIPC has determined that there is no valid purpose under FIPPA supporting the collection of the personal information through the PSCS. With no authorized purpose existing under FIPPA, the condition of "consistent purpose" under s. 33(2)(d) cannot be met as there is no authorized purpose for the disclosure to be consistent with.

Section 33(2)(l)

Under s. 33(2)(l), a public body may also disclose personal information to comply with a subpoena, warrant or court order. The City advised that it does not anticipate any such requests for information will take place throughout the duration of the field test and, to date, no such disclosure has occurred under s. 33(2)(l). However, it is possible that, should a subpoena, warrant, or court order be produced during the time of the field test, the City would be required to disclose the personal information at issue.

Sections 5 and 3(5)

The City stated that PSCS field test footage would not be disclosed to the public, for example, through a FOI request under s. 5[61], or as a record for purchase (as is currently done with CCTV traffic footage).[62] The City noted that any FOI requests made throughout the duration of the field test would likely be made too late due to the 48-hour retention period. Alternatively, the City noted that, if requested, such records would likely be withheld under ss. 22 (disclosure harmful to personal privacy) or s. 15 (disclosure harmful to law enforcement) of FIPPA.[63]

As the overall collection of personal information through the PSCS is not authorized by ss. 26(b) or (c), the City is unable to rely on s. 26(e). **Therefore, the City is not authorized to disclose the personal information it has already collected during the field test except under limited circumstances, such as the production of a subpoena, warrant or court order under s. 33(2)(l) or a request for one's own personal information under s. 5.**

61. See FIPPA, s. 3(5)(a).

62. https://www.richmond.ca/services/transportation/videorequest.htm.

63. Whether these sections would be appropriately applied would depend on a case-by-case basis and would be subject to OIPC review should the applicant request it.

DUTY TO PROTECT

While the City is not authorized to collect, use, or disclose personal information through the PSCS field test, it has already collected personal information throughout the field test. As such, the City is still required under s. 30 to protect personal information in its custody or under its control.

The OIPC did not physically inspect the City's PSCS security. However, **based on the City's representations, the OIPC is satisfied that the City has a reasonably robust set of security controls in place to protect recorded footage and personal information captured during the field test.** Regardless, as outlined in Recommendation 2, the City is to immediately delete all PSCS recordings.

A summary of the safeguards employed by the City is included for information purposes.

Access control

The City advised that physical access to cameras, network cables and switches located at the field location are restricted to authorized Traffic personnel employed by the City. Additionally, PSCS cameras are mounted on metal poles supporting the traffic signals and positioned out of easy reach. The cables are enclosed within these poles and cable connections and switches are housed inside a tamper-proof traffic cabinet. Cameras and the network switches at the field location can only be access by authorized Traffic personnel.

The PSCS network switches, servers, and storage devices are physically secured in City Data Centre facilities and access is restricted to the IT infrastructure team and logged in the facility's access card system. The PSCS network infrastructure is isolated from other city infrastructure and has no Internet access. There is a formal Access Authorization process to ensure only approved personnel can get access and robust authentication is required (based on having a token/passkey) to access the system. The City utilizes robust access management software and a managed security service provider to control and monitor accesses.

The City also advised that vendor-supported configurations or troubleshooting by Genetec are conducted through a supervised secured remote access session. These sessions are initiated only with explicit authorization from the Business Analysis team in the IT Department and are monitored to prevent unauthorized actions.

There is a formal change management process in place to ensure only authorized changes are made to network switches, servers, and storage devices. Change requests documenting the change details, risks, and impacts are submitted and all change requests are reviewed and approved by the Change Review Committee.

Activity monitoring

The City advised that system monitoring is performed at both the network/firewall level and server level using industry standard security applications. The systems generate alerts that are sent to a Cybersecurity Incident Response Team (CSIRT), a designated group of staff members, including senior management. All access to the VMS server is provided through, and monitored by, a robust privileged access management system. This allows specific members of the CSIRT to have authorized access as and when required.

Incident response

The City has demonstrated a robust Cyber Incident Response Plan (IRP) is in place and a CSIRT has been identified. Further, the City conducted a tabletop exercise in April 2025, testing the IRP.

Data encryption

The PSCS VMS utilizes standard Internet Transport Layer encryption (TLS protocol) to protect video data from the camera to the server. The VMS then uses the encryption feature built into the Database Management Service (MS SQL) that it uses to store and provide access to the data. This is reasonably robust way to prevent unauthorized access to the information.

The City advised that the Genetec Security Center uses certificates, digital signatures, and encryption protocols to protect data. It encrypts all video in transit when it enters the premises until it is viewed by the user. This protection can be extended to encrypt video in transit from cameras for compatible devices. Backups are stored at the protected and restricted storage array in the Data Centre at the City Hall and Works Yard.

Encryption helps to protect outgoing data or data in transit, hides data from people not authorized to view it, and protects the confidentiality of data stored on a computer or communicated over a network. Genetec Security Center leverages Microsoft SQL databases. Microsoft SQL offers data encryption via Transparent Data Encryption, and this option protects the data at rest.

Data transfer

The City has yet to determine a formal data transfer process but planned to evaluate this as part of the PSCS field testing. The City stated that further consultation with the Richmond RCMP would be required to determine a secured data transfer process.

DISCUSSION

DISCOURSE ON PUBLIC SURVEILLANCE FOR LAW ENFORCEMENT PURPOSES

Public sentiment on the City's initiative

The City is required to give public notice of its meetings, and provide agendas and reports related to items on the agenda to the public. After the City gives notice, members of the public may attend Council and Committee meetings to discuss agenda items and any related concerns.

The City provided two examples where the public had the opportunity to discuss and raise concerns about the PSCS. The first was at the City's December 2, 2024, General Purposes meeting when the report titled "Phasing Options for the Public Safety Camera System" was presented.[64] The second was at the March 11, 2025, Community Safety Committee meeting, where a member of the public expressed concerns with the installation of high-resolution cameras at intersections, including:

- privacy issues for residents;
- the OIPC's recommendations to the City to not move forward with the cameras;
- studies in the UK that did not provide sufficient evidence that cameras reduce crime;
- whether the cameras will enhance public safety;
- data storage and access; and
- whether the City examined less invasive options.[65]

A member of the public started an online petition against the City's use of high-resolution cameras for PSCS. At the time of reporting, this petition collected 47 signatures and 19 comments were posted, mostly expressing views opposing the City's plan to install high resolution cameras at City intersections.[66]

Additionally, journalists and media have long reported on the City's ongoing interest to install high-resolution cameras at intersections – with responding public commentary representing mixed views, some supporting and some objecting to the cameras. In one example, media critically reported that, in 2021, the City asked the Provincial Government for an exemption under FIPPA to allow it to install and use high resolution cameras for criminal investigation and

64. City of Richmond General Purposes Meeting Agenda. December 2, 2024. https://citycouncil.richmond.ca/agendafiles/Open_GP_12-2-2024.pdf.
65. City of Richmond Community Safety Committee Meeting Minutes. March 11, 2025. https://citycouncil.richmond.ca/agendas/safety/031125_minutes.htm.
66. Stop 4K High-resolution cameras from being installed at intersections in Richmond, BC. https://www.openpetition.org/ca/petition/online/stop-4k-high-resolution-cameras-from-being-installed-at-intersections-in-richmond-bc#petition-main.

prosecution.[67] In other more recent examples, local media covered the City's actions to revisit the use of high-resolution cameras, including council members' and public's concerns over privacy and legality, as well as cost, necessity, and effectiveness.[68] [69] [70] [71] [72] [73]

Broader public sentiment on video surveillance

As video surveillance technology has improved and the price of data storage has declined in recent years,[74] various jurisdictions have explored expanding their use of surveillance cameras for law enforcement purposes. To date, studies on the effectiveness of surveillance cameras have mainly focused on crime prevention and deterrence, with mixed results.[75] [76] Certain contexts, such as the use of CCTV in parking garages and residential areas, equipped with live monitoring, and cameras used in conjunction with other techniques and technologies, appear to be more successful than others.[77]

However, crime rates are complex and reasons for fluctuations can hardly be distilled to any one factor or technology. In instances where crime reduction has been evidenced, effects have been modest and limited to certain types of activity, for example, vehicle and property crimes.[78]

---

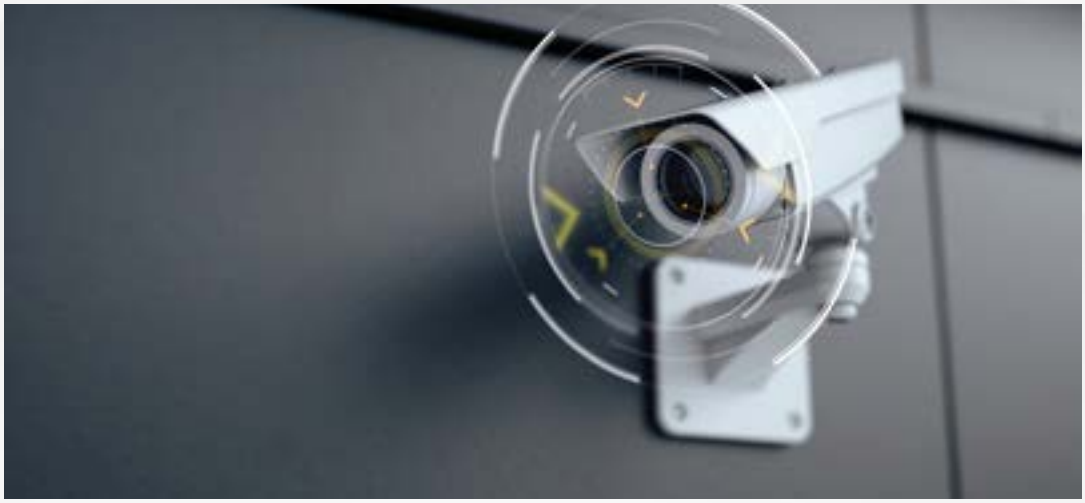
67. Bramham, D. 2021, May 28. There's a world of difference between monitoring and spying. The Vancouver Sun (online). https://vancouversun.com/opinion/columnists/daphne-bramham-theres-a-world-of-difference-between-monitoring-and-spying.
68. Rantanen, M. 2023, September 12. Richmond council challenges privacy commissioner's ruling on traffic cameras. Richmond News (online). https://www.richmond-news.com/local-news/richmond-council-challenges-privacy-commissioners-ruling-on-traffic-cameras-7539380.
69. Rantanen, M. 2023, December 15. High-resolution traffic cameras in Richmond could cost up to $6.5 million. Richmond News (online). https://www.richmond-news.com/local-news/high-resolution-traffic-cameras-in-richmond-could-cost-up-to-65-million-7986582.
70. Bell, A. 2024, January 16. Interview with Michael Wolfe, Richmond Councillor. On the Coast, CBC Vancouver.
71. Rantanen, M. 2024, November 26. Cameras for police use proposed at 10 Richmond intersections. Richmond News (online). https://www.richmond-news.com/local-news/cameras-for-police-use-proposed-at-10-richmond-intersections-9866101.
72. Rantanen, M. 2024, December 11. Two Richmond councillors oppose 2025 budget. Richmond News (online). https://www.richmond-news.com/local-news/two-richmond-councillors-oppose-2025-budget-9943057.
73. Piao, J., Millar, K. et al. 2025, February 22. Letters: Richmond News reader raises concerns about 'mass surveillance' with CCTV cameras. Richmond News (online). https://www.richmond-news.com/opinion/letters-richmond-news-reader-raises-concerns-about-mass-surveillance-with-cctv-cameras-10273289.
74. Office of the Privacy Commissioner of Canada. 2006. Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/vs_060301/
75. Webster, C. W. R. 2009. CCTV policy in the UK: reconsidering the evidence base. Surveillance & Society 6(1): 10-22. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3400.
76. Carr, R. 2016. Political Economy and the Australian Government's CCTV Programme: An Exploration of State-Sponsored Street Cameras and the Cultivation of Consent and Business in Local Communities. Surveillance & Society14(1): 90-112. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/pe-cctv.
77. Thomas, A. L., Piza, E. L., Welsh, B. C., & Farrington, D. P. 2022. The internationalisation of cctv surveillance: Effects on crime and implications for emerging technologies. International journal of comparative and applied criminal justice, 46(1), 81-102. https://www.tandfonline.com/doi/full/10.1080/01924036.2021.1879885.
78. Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. 2019. CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology & public policy, 18(1), 135-159. https://doi.org/10.1111/1745-9133.12419.

Few studies have evaluated the effectiveness of CCTV in Canada, and further research is needed on the effectiveness of CCTV as an investigative tool more generally. The OIPC has pointed to a lack of evidence regarding video surveillance effectiveness several times over the last two decades.[79] These are important considerations when weighing the necessity of collection against the volume and sensitivity of the information collected and proportional expected outcomes.

Mixed results and limited evidence of effectiveness combined with the public's privacy concerns about the right to be let alone have often led to controversial debates regarding the use of CCTV for law enforcement. There are several barriers that tend to factor into the discussion.

For example, in 2018, the City of Vancouver contemplated installing a network of surveillance cameras in the Granville Entertainment District (GED) for deterring and investigating violent crime and property crime. Ultimately, the City Manager cited:

1. the City of Vancouver's inability to meet FIPPA requirements that would authorize it to collect personal information for law enforcement purposes;
2. a lack of clear evidence of effectiveness; and
3. cost, as the reasons for the program would not be moving forward.[80]



79. "In 2001, then privacy commissioner David Loukidelis reported that pervasive use of video surveillance had little or no effect on reducing crime. Nothing has changed since then. We must learn from the experience in other jurisdictions, such as the UK, where over 6 million cameras (one for every ten people) have not significantly reduced crime in urban centres". Use of Video Surveillance by Local Governments. OIPC to City of Vancouver. 2018. p. 14. https://vancouver.ca/files/cov/2018-04-27-cctv-use-in-the-granville-entertainment-district.pdf.

80. "From all of the information and input obtained to date, it appears that the City of Vancouver would be unable to meet the statutory requirements imposed by FIPPA to conduct regular video surveillance of the public realm in the GED, where the stated purpose of such surveillance is the deterrence and investigation of property and violent crime. Given the foregoing, as well as the unclear evidence of efficacy in the particular circumstances of the GED and cost implications, City staff do not recommend proceeding with the installation of CCTV in the GED at this time". City of Vancouver. p. 14. https://vancouver.ca/files/cov/2018-04-27-cctv-use-in-the-granville-entertainment-district.pdf.

Other jurisdictions have come to similar conclusions.[81] Related capabilities (e.g. FRT) licence plate scanning, etc.) have also prompted critical discussions around their appropriate use for policing communities. Considerations often include, but are not limited to, the importance of preserving democratic values such as privacy,[82] institutional accountability and transparency over how new and existing systems are used,[83] the potential for bias or selective surveillance and/or policing against certain communities,[84] and levels of effectiveness of video surveillance systems for crime deterrence or law enforcement investigations.[85]

Other recent examples have pointed to a lack of transparency and accountability regarding which surveillance tools are being used, by whom, for which purposes, and have resulted in public outcry or controversy. For example, the RCMP previously relied on FRT for hundreds of searches through Clearview AI.[86] A joint investigation by the Office of the Privacy Commissioner of Canada (OPC) alongside the OIPC and other provincial privacy offices found Clearview AI to have illegally compiled a database of images by scraping social media data.[87]

Further, complaints from civil liberties groups have pointed to a growing culture of police surveillance and unclear policies regarding the usage of drones and smart phones for video surveillance of political protests in Vancouver.[88] A lack of accountability or transparency around how surveillance tools are used by law enforcement can result in a lack of trust in public sector institutions. This is also concerning as surveillance in public more generally can lead to a chilling effect on democratic participation.[89]

---

81. Relatedly, in 2020, the Ottawa Police decided against implementing a CCTV camera project following an internal document acknowledging the lack of evidence in effectiveness for law enforcement practices. See Cave, D. 2022. Safety in Cameras? – An Exploratory Study of the Ottawa Public Surveillance (CCTV) Project. Carleton MA thesis. 1-257. https://carleton.scholaris.ca/items/2f04d55c-13c7-44f0-a565-e161bc39b6bf/full.

82. "Finally, I trust that the City will consider the experience in other jurisdictions, such as Seattle, where that City Is spending over $150,000 to dismantle a multi-million dollar mesh network of wireless and CCTV that was never activated due to privacy concerns of its citizens." OIPC to City of Vancouver. March 13, 2018. P. 20.

83. Taylor, N. 2011. A Conceptual Legal Framework for Privacy, Accountability and Transparency in Visual Surveillance Systems. Surveillance & Society 8(4): 455-470. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4182.

84. Hendrix, J. A., Taniguchi, T. A., Strom, K. J., Barrick, K. A., & Johnson, N. J. 2018. The eyes of law enforcement in the new panopticon: Police-community racial asymmetry and the use of surveillance technology. Surveillance & Society, 16(1), 53-68. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6709.

85. Thomas, A. L., Piza, E. L., Welsh, B. C., & Farrington, D. P. 2022. The internationalisation of cctv surveillance: Effects on crime and implications for emerging technologies. International journal of comparative and applied criminal justice, 46(1), 81-102. https://www.tandfonline.com/doi/full/10.1080/01924036.2021.1879885.

86. Tunney, C. 2021. 2021, June 10. RCMP's Use of Facial Recognition Tech Violated Privacy Laws, Investigation Finds. CBC (online). https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.6060228.

87. Office of the Privacy commissioner of Canada (2021). Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta https://www.oipc.bc.ca/documents/investigation-reports/2357.

88. British Columbia Civil Liberties Association. 2024. Service and Policy Complaint – VPD Surveillance of Demonstrators Supporting Palestinian Human Rights. September 18, 2024. https://assets.nationbuilder.com/pivotlegal/pages/3738/attachments/original/1726622087/Surveillance_Complaint_September_18__2024.pdf?1726622087.

89. "Individuals may alter or censor their activities when they are aware of being watched and feel inhibited from participating in lawful activities such as accessing medical services, protesting peacefully or advocating for societal change. ALPR systems

Next, the potential for bias against certain communities in the deployment of policing or surveillance technologies is an oft-cited reason for limiting surveillance. Recent studies have uncovered a link between acceptance attitudes around the increased culture of surveillance in general, regarding normalized practices from the private sector, and domestic policing surveillance. However, researchers suggest individuals should make careful distinctions between the implications of private sector surveillance and domestic police surveillance. Domestic police surveillance arguably leads to more serious equity and social justice implications, especially for marginalized groups.[90]

Similar arguments were made in 2022, for instance, when Vancouver City Council rejected a motion to expand CCTV usage in public spaces, councillors cited public concerns around further criminalizing people living in poverty, among related issues.[91] Across Canada and in British Columbia, Indigenous groups and people of colour are subject to over-policing and disproportionate levels of surveillance relative to their population sizes.[92] [93] [94] [95]

For reasons such as these, various jurisdictions across North America and Europe have debated the extent to which video surveillance technologies should be used and/or expanded upon, particularly with apprehensions respecting racial bias in implementation and law enforcement, especially in relation to predictive policing algorithms and FRT.[96] [97] [98]

---

have the potential to cause unintended consequences, such as a chilling effect on freedom of speech and association." See Information and Privacy Commissioner of Ontario. 2024. Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services. https://www.ipc.on.ca/en/media/5059/download?attachment.

90. Conrey, C., & Haney, C. 2024. Understanding attitudes toward police surveillance: The role of authoritarianism, fear of crime, and private-sector surveillance attitudes. Surveillance & Society, 22(4), 428-447. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/17177.

91. Little, S. 2022, April 27. Vancouver City Council Rejects Use of CCTV Cameras To Combat Crime. Global News (online). https://globalnews.ca/news/8791322/vancouver-cctv-public-safety-debate/.

92. African Art & Cultural Community Contributor CCC Inc. / Issamba Centre. 2022. Black in BC. Convener Pilot Project. https://www.issambacentre.ca/_files/ugd/dc8154_6a54db5be2a9432ba07129e03b953784.pdf

93. BC's Office of the Human Rights Commissioner (2021). Equity is safer: Human rights considerations for policing reform in British Columbia. https://bchumanrights.ca/resources/publications/publication/scorpa/.

94. R. v. Le, 2019 SCC 34 (CanLII), [2019] 2 SCR 692, <https://canlii.ca/t/j0nvf>, para 97.

95. Dawson, F. 2021, November 24. Systemic racism within British Columbia police targets minorities. The Star (online). https://www.thestar.com/news/canada/systemic-racism-within-british-columbia-police-targets-minorities/article_bc6ffa3e-d7aa-5d39-a042-660119fbee68.html.

96. Conrey, C., & Haney, C. 2024. Understanding attitudes toward police surveillance: The role of authoritarianism, fear of crime, and private-sector surveillance attitudes. Surveillance & Society, 22(4), 428-447. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/17177.

97. American Civil Liberties Association. 2016. Community Control Over Police Surveillance: Technology 101. https://www.aclu.org/publications/community-control-over-police-surveillance-technology-101.

98. Hendrix, J. A., Taniguchi, T. A., Strom, K. J., Barrick, K. A., & Johnson, N. J. 2018. The eyes of law enforcement in the new panopticon: Police-community racial asymmetry and the use of surveillance technology. Surveillance & Society, 16(1), 53-68. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6709.

Overall, public perception and controversy related to domestic policing surveillance programs can often be linked to the following factors:

- the need for individual or group privacy in public places to protect civil liberties including the values of dignity, integrity and autonomy;[99]
- historical issues with transparency and accountability regarding how surveillance tools are used and for which purposes;
- the disproportionate negative effects of surveillance and policing on certain groups, which is not exclusive to any one technology or practice in particular;
- necessity of the information collected in proportion to the issue to be solved; and
- the effectiveness of video surveillance programs and related technology relative to their cost.

Taken together, these factors create the backdrop for what a public body should consider when evaluating any new, proposed, or expanded surveillance program – especially for the purposes of law enforcement, such as the City's field test.

Although the City explained that the field test is limited to select areas for very limited purposes (and will not include FRT or be deployed to monitor protests, for example), the program still collects the personal information of tens of thousands of individuals on a daily basis. It remains uncertain how the RCMP would use the footage or images collected by the City, should the PSCS be fully implemented or whether additional capabilities could be incorporated later.

As technological capabilities continue to improve, the potential for function creep should always be acknowledged by public bodies when considering collecting personal information.

As explained by former Commissioner Denham in a previous report on the use of facial recognition, the potential for function creep is important to consider because it is linked to the fundamental privacy principle of using personal information only for purposes it was collected. Considering the possibility for function creep is essential in cases where biometric identification could potentially later be involved because of the implications of identifying individuals in public:

> With the implementation of facial recognition individuals will no longer be able to remain anonymous in public places. The system may, in a matter of seconds to minutes, identify you to the public body or organization running the facial recognition software. Previously private political, religious and social affiliations will now become public.[100]

That said, the PSCS does not use FRT software at present. Finally, as the OIPC can only

99. R. v. Plant, 1993 CanLII 70 (SCC), [1993] 3 SCR 281, <https://canlii.ca/t/1fs0w>, page 292.
100. OIPC BC. February 2012. Investigation Report F12-10: *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia.* https://www.oipc.bc.ca/investigation-reports/1245.

investigate cases where personal information is already being collected, used, or disclosed, this report focuses on the limited application of the field test and not the full implementation phase or any later possible phases of the project. These considerations simply provide the backdrop for further thinking and discourse about the potential broader implications of such a program.

In addition, it is important to consider the fact that at least one of the PSCS cameras does have FRT features available. Although the City chose not to utilize FRT during the field test, cameras with such features are easy to acquire from organizations such as Genetec. Other public bodies or other entities may be tempted to purchase similar technology for a range of purposes.

The OIPC has made several recommendations regarding biometric data collection, such as through FRT, by the private sector.[101] A recent report on Canadian Tire's use of FRT recommended that BC's private sector privacy legislation, the *Personal Information Protection Act* (PIPA), be amended to include specific obligations regarding the collection, use or disclosure of biometric information, including requiring notification to the OIPC. This would modernize legislation as other jurisdictions, such as Quebec, already have.[102]

To date, aside from abovementioned investigation reports into Clearview AI and ICBC's use of FRT for assisting law enforcement, little has been written concerning biometric surveillance by public bodies in BC.

In 2022, the Office of the Privacy Commissioner (OPC) worked with provincial privacy commissioners to produce *Privacy Guidance on Facial Recognition for Police Agencies*[103] which makes several additional contributions relevant to this discussion:

- Mass surveillance is often associated with societal harms such as disproportionate negative impacts for racialized and other marginalized groups, which can be further exacerbated by sophisticated technologies such as FRT.
- Inappropriately used surveillance technology can have long-lasting effects on privacy rights that can be difficult to dial back or remedy once already in place.
- Outside of Quebec, appropriate regulatory limits on FRT have yet to be implemented, in ways that create confusion over appropriate use: "… its use is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed by FR. This creates room for uncertainty concerning what uses of FR may be acceptable, and under what circumstances."[104]
- It is not clear where the acceptable use of FRT "begins and ends", a question which is essential to the future of privacy protection across Canada.

101. OIPC BC. April 2023. Investigation Report 23-02: Canadian Tire Associate Dealers' use of facial recognition technology. https://www.oipc.bc.ca/documents/investigation-reports/2618.
102. This report also recommended regulation of the sale or installation of technologies that capture biometric information.
103. Office of the Privacy Commissioner of Canada. 2022. Privacy Guidance on Facial Recognition for Police Agencies. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/.
104. Ibid.

Because of the ready availability of sophisticated surveillance technology to those seeking it, the potential for misuse and harm, and the relative uncertainty regarding the legal limits of biometric surveillance, the OIPC recommends that the BC Government regulate technologies that capture biometric information.

Recommendation 4

The BC Government should regulate, through legislative amendment, technologies that capture biometric information.

CONCLUSION

The purpose of this report has been to establish whether the City of Richmond has the authority to collect, use or disclose personal information through its PSCS field test and whether the collected information has been adequately secured. While the OIPC found no concerns with the security controls, the PSCS field test is not authorized under FIPPA and the OIPC recommended that the City immediately stop collecting personal information through the field test, delete the recordings, and disband the cameras.

The City advised that it did not intend to comply with the recommendations, and the Commissioner issued an Order on this matter. Other public bodies considering similar surveillance programs should review this report and findings, along with the Order, for guidance before initiating such programs. Regardless of whether a municipality has its own police department or uses the RCMP, the same analysis would apply.

Public surveillance has remained a controversial issue for the last three decades. Public bodies may be tempted to rely on enhanced technological capabilities of video cameras, especially those that come equipped with facial recognition, licence plate recognition, gunshot detection, and other such features. However, considerations should be made surrounding the legality, effectiveness, and the privacy impacts of video surveillance cameras and the associated tools they now come equipped with.

Limits on public surveillance are embedded into law to protect the privacy rights of individuals. The research shows that the overall effectiveness of such programs are mixed and contingent on the context such as whether video is live-monitored, the type of crime, and the environment. At the same time, the disproportionate negative impacts on disadvantaged groups and individuals have been well documented, not to mention the potential civil society implications. Programs that collect information on everyone in an effort to police a few individuals are rarely justified, as the collective privacy impacts are not proportional to the anticipated benefits.

Where possible, public bodies should aim to use more effective and less invasive measures to meet their goals. Further, public bodies who do not have a law enforcement mandate need to consider whether and how public surveillance may be authorized.

Finally, while such features were disabled in this case, the widespread availability of AI-enabled surveillance tools is a cause for concern. The sale of surveillance tools with AI-enabled capabilities, such as those that collect biometrics like facial recognition, should be explicitly regulated to ensure appropriate guardrails are in place to avoid over stepping of the limits or the potential misuse of such tools.

Acknowledgement

I thank the City of Richmond for participating in this investigation, responding to questions, and collecting and providing the requested documents and materials.

I would also like to thank my staff, in particular, Jessica Percy Campbell, Investigator; Gary Freeburn, Compliance Auditor; and Tanya Allen, Director of Audit and Systemic Review for conducting this investigation and drafting this report.

RECOMMENDATIONS

Recommendation 1

The City should immediately stop collecting personal information through the PSCS.

Recommendation 2

The City should immediately delete all PSCS recordings to date.

Recommendation 3

The City should disband PSCS equipment used to collect personal information.

Recommendation 4

The BC Government should regulate, through legislative amendment, technologies that capture biometric information.

RESOURCES

Getting started

- Access to data for health research
- BC physician privacy toolkit
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Guide to OIPC processes (FIPPA and PIPA)
- Guide to PIPA for business and organizations
- Privacy impact assessments for the private sector
- Privacy management program self-assessment

Access (General)

- Common or integrated programs or activities
- Guidance for conducting adequate search investigations (FIPPA)
- Guidance on FIPPA's FOI process
- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- PIPA and workplace drug and alcohol searches: a guide for organizations
- Proactive disclosure: guidance for public bodies
- Requesting records of a deceased individual
- Section 25: The duty to warn and disclose
- Time extension guidelines for public bodies
- Tip sheet: requesting records from a public body or private organization

Privacy (General)

- Direct-to-consumer genetic testing and privacy
- Disclosure of personal information of individuals in crisis
- Employee privacy rights
- Guide for organizations collecting personal information online
- Identity theft resources
- Information sharing agreements
- Instructions for written inquiries
- Obtaining meaningful consent
- Political campaign activity code of practice
- Political campaign activity guidance
- Privacy guidelines for strata corporations and strata agents
- Privacy-proofing your retail business
- Privacy tips for seniors: protect your personal information
- Private sector landlord and tenants
- Protecting personal information away from the office
- Protecting personal information: cannabis transactions
- Reasonable security measures for personal information disclosures outside Canada
- Responding to PIPA privacy complaints
- Securing personal information: A self-assessment for public bodies and organizations

Comprehensive privacy management

- Accountable privacy management in BC's public sector
- Getting accountability right with a privacy management program

Privacy breaches

- Privacy breaches: tools and resources for public bodies
- Privacy breach checklist for private organizations
- Privacy breach checklist for public bodies
- Privacy breaches: tools and resources for the private sector

Technology and social media

- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for conducting social media background checks
- Mobile devices: tips for security & privacy
- Tips for public bodies and organizations setting up remote workspaces
- Use of personal email accounts and messaging apps for public body business

Infographics

- FIPPA and the application fee
- How to identify deceptive design patterns
- How to make a complaint
- How to make an access request
- How to request a review
- Identifying and mitigating harms from privacy-related deceptive design patterns
- Responsible information sharing in situations involving intimate partner violence
- Requesting records of deceased individuals
- Tips for requesting records
- Transparency by default: information regulators call for a new standard in government review
- Tip sheet: 10 tips for public bodies managing requests for records

oipc

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4

Telephone: 250.387.5629
Toll Free in BC: 1.800.663.7867

Email: info@oipc.bc.ca

oipc.bc.ca