Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MI18-5

The City of Cambridge

April 23, 2021

Summary: The Office of the Information and Privacy Commissioner of Ontario received a privacy complaint involving the City of Cambridge (the city). The complaint was about the city's installation of a video surveillance system in its downtown core areas. The complainant was concerned that the city's operation of the system breached the privacy of individuals under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

This report finds that the city has not conducted an assessment of whether the video surveillance system is necessary to achieve its objectives and recommends that it do so, to ensure compliance with the *Act*.

In the event that the city's assessment determines that the system is necessary and the collection of personal information is thus consistent with the *Act*, this report considers whether the city's notice of collection and use and disclosure of the personal information is in accordance with the *Act*. It also considers whether the city provides a right of access to this information, as well as whether the city has reasonable privacy protection measures and retention periods in place.

This report finds that the city's notice of collection and use and disclosure of the personal information is in accordance with the *Act*. It also finds that there is a right of access to this information and that the city has reasonable protection measures and proper retention periods in place.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy* Act, R.S.O. 1990, c. M. 56, as amended, ss. 2(1), 28(2), 29(2), 30(1), 31, 32(a), (d), (g) and (h) and 36(1); *Municipal Act, 2001* S.O. 2001, c. 25, as amended, section 11(1); and *R.R.O. 1990*, Regulation 823, as amended, sections 3(1) and 5.

Orders and Investigation Reports Considered: Privacy Investigation Report MC07- 68; Privacy Complaint Reports MC13-46, MC13-60, MC17-32 and PR16-40; and Investigation Report I93-044M.

OVERVIEW:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a privacy complaint under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) about the City of Cambridge (the city)'s installation of video surveillance cameras in the Galt Core Area[1].

[2] The complaint alleged that the city's operation of the cameras breached the privacy of individuals under the *Act* and that they had been installed without a policy in place governing their usage.

[3] To address the matter, the IPC opened a Commissioner-initiated privacy complaint file and commenced an investigation to review the city's practices relating to its video surveillance system.

[4] In response, the city, which has a population of over 129,000 people[2], provided this office with detailed information about its video surveillance system, as well as other relevant information discussed below. The city also provided a copy of its "Surveillance Cameras in the Downtown Core Areas" policy (the Surveillance Policy).[3]

BACKGROUND:

Video Surveillance Camera Installations

[5] In 2017, to enhance a positive and safe environment for the city's (downtown) Core Areas[4], the city's council approved Phase 1 of its security camera project (the Camera Project).

[6] In March 2018, as part of Phase 1 of the Camera Project, the city installed ten (10) external video surveillance cameras at 10 different locations consisting of

---

[1] The Galt Core is one of the city's Core Areas. See https://www.cambridge.ca/en/learn-about/Downtown-Development-and-Revitalization-Core-Areas.aspx
[2] https://www.investcambridge.ca/en/why-cambridge/demographics.aspx#
[3] This policy, effective September 18, 2019, is the updated version of the city's "Surveillance Cameras in the Cambridge Core Areas" policy that was effective May 15, 2018. The policy is available at: https://www.cambridge.ca/en/your-city/resources/Policies---Video-Surveillance-System.pdf
[4] https://www.cambridge.ca/en/your-city/resources/2018-05-15_18-021OCM-Policies---Video-Surveillance-System.pdf

intersections, lots, parking lots and streets in the city's Core Areas.[5]

[7] In May 2018, before any of the video surveillance cameras began recording, the city's council approved the Surveillance Policy pursuant to its Staff Report No: 18-021 OCM (the Staff Report).[6]

[8] The Staff Report's Executive Summary explains that its purpose was to request that the city's Council approve the Surveillance Policy prior to the activation of the Surveillance Cameras. To that end, the Staff Report provides background information about Phase 1 of the Camera Project and discusses how this project strategically aligns with the city's goal of a safe and vibrant downtown Core Area.

[9] Further, the Staff Report contains reasons for the Surveillance Policy, information about other initiatives that have been implemented to achieve the city's goal, as well as, with respect to the project, information about the application of the *Act*, financial impact, public input and internal and external consultation. In conclusion, this report recommended that the city Council approve the Surveillance Policy.

[10] In September 2018, the city's council approved Phase 2 of the Camera Project. As part of Phase 2, between September 2019 and December 2019, one camera was installed at the end of the Water Street Pedestrian Bridge and five cameras were installed along the Dan Spring Way Trail.[7]

[11] According to the city, all of the cameras installed were on the property of the Grand River Conservation Authority[8] (GRCA) and the city.

[12] The city advised that video recording began in July 2018 and December 2019, respectively, for the cameras installed in Phase 1 and in Phase 2. The city also advised that all of the cameras record 24 hours a day, 7 days a week and that, in accordance with the Surveillance Policy, "signs are posted at public access points to and within areas under surveillance."

The Surveillance Policy

[13] The Surveillance Policy "applies to municipal video surveillance systems located

---

[5] The Surveillance Policy defines "Cambridge Core Areas" as the core areas as established by Maps 3, 4 and 5 in the city's Official Plan, namely the Galt City Centre, the Preston Towne Centre, and Hespeler Village, respectively. For detailed information about the camera locations, see section 3.2. of Schedule B to the Surveillance Policy.

[6] https://www.cambridge.ca/en/your-city/resources/2018-05-15_18-021OCM-Policies---Video-Surveillance-System.pdf

[7] Section 3.2. of Schedule B to the Surveillance Policy

[8] The GRCA is a partnership representing watershed municipalities. The city is one of these municipalities. See https://www.grandriver.ca/en/who-we-are/GRCA-partners.aspx

in the [city's] Core Areas" and to "all [of the city's] employees, including full-time, part-time, casual, contract, volunteer and co-op placement employees."

[14] This policy defines "video surveillance system" as "a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in public spaces or within City operated facilities."

[15] It also makes it clear that the city "is responsible for the video surveillance systems and maintaining custody and control of video records at all times on City property."

DISCUSSION:

[16] The following addresses whether the city's video surveillance system is in accordance with the privacy protection rules set out in the *Act* relating to the collection, notice, use, disclosure, security and retention of personal information.

[17] In this report, I will refer to the IPC's *Guidelines for the Use of Video Surveillance* (the Guidelines).[9] The Guidelines set out best practices for institutions to follow when implementing a video surveillance system.

ISSUES:

[18] I identified the following issues as arising from this investigation:

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?
2. Is the collection of the personal information in accordance with section 28(2) of the *Act*?
3. Is the notice of collection in accordance with section 29(2) of the *Act*?
4. Is the use of the personal information in accordance with section 31 of the *Act*?
5. Is the disclosure of the personal information in accordance with section 32 of the *Act*?

---

[9] https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf

6. Is there a right of access to the personal information in accordance with section 36(1) of the *Act*?

7. Are there reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*?

8. Does the city have proper retention periods in place for the personal information?

Issue 1: Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

[19] The information at issue is the images of identifiable individuals collected by the city's video surveillance system.

[20] "Personal information" is defined in section 2(1) of the *Act*, in part, as follows:

> "personal information" means recorded information about an identifiable individual, including,
>
> > (a) information relating to the race, national or ethic origin, colour, religion, age, sex, sexual orientation or martial or family status of the individual,

[21] Previous decisions by this office have held that information collected about identifiable individuals by video surveillance systems qualifies as "personal information" under the *Act*.[10] The city does not dispute this.

[22] Further, the Surveillance Policy states:

> Since images of individuals collected by this video surveillance system are considered to be the personal information of the individuals photographed the recordings are subject to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).[11]

[23] Based on the above, I find that the information at issue qualifies as "personal information" under section 2(1) of the *Act*.

---

[10] Privacy Investigation Report MC07-68 and, Privacy Complaint Reports MC10-2, MC13-46 and MC13-60, all available at: https://decisions.ipc.on.ca/ipc-cipvp/en/nav.do
[11] Section 1.3 of Schedule B to the Surveillance Policy

Issue 2: Is the collection of the personal information in accordance with section 28(2) of the *Act*?

[24] Section 28(2) of the *Act* requires that the city's video surveillance system collect the personal information only in certain circumstances. This section states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[25] The city advised that, pursuant to section 11(1) of the *Municipal Act, 2001* (the *Municipal Act*)[12], the collection of the personal information at issue is necessary to the proper administration of a lawfully authorized activity.

[26] Accordingly, first, the city must show that the activity is lawfully authorized and, second, that the collection is necessary to the proper administration of that activity.

[27] Section 11(1) of the *Municipal Act* states:

> A lower-tier municipality and an upper-tier municipality may provide any service or thing that the municipality considers necessary or desirable for the public, subject to the rules set out in subsection (4).

[28] The city advised that the lawfully authorized activity is the city's operation of the Core Areas, that is, the city's provision of intersections, lots, parking lots, streets, a bridge and trail within these areas, which under section 11(1) of the *Municipal Act*, the city "considers necessary or desirable for the public".

[29] I accept the city's position in this regard and, therefore, I am satisfied that the city's operation of the Core Areas is a lawfully authorized activity.

[30] Next, I must consider whether the collection of the personal information through the city's video surveillance system is necessary to the proper administration of its operation of the Core Areas.

[31] In *Special Investigation Report* MC07-68, then Commissioner Ann Cavoukian set out what the necessity condition means as follows:

> Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the "lawfully authorized activity" in question, and second, it must

---

[12] S.O. 2001, c.25

> demonstrate how the collection of personal information is "necessary," not merely helpful, to the achievement of this objective. In addition, this justification must be provided for all classes of personal information that are collected.[13]

[32] Moreover, in the context of video surveillance, the Guidelines discusses the importance of considering the necessity condition with respect to the means used to collect the personal information, as well as the sensitivity and the amount of the personal information collected.[14]

[33] Regarding the means used to collect the personal information, the Guidelines advise that it is important that institutions consider whether:

- 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.

[34] The city advised that there is a real, substantial and pressing problem of public safety to be addressed by its video surveillance system. As evidence of this concern, the city advised that there are police reports documenting incidents that have occurred in the Core Areas.

[35] In 2018, as less intrusive means to address public safety concerns, the city advised that it implemented its Ambassador Program.[15] The goals of this program are to enrich the downtown experience in the city, keep the Core Areas clean and well-maintained, and enhance the safe enjoyment and pride in the community.

[36] Members of the Ambassador Program provide safety and security in the Core Areas by having a visible presence, regularly patrolling busy areas, requesting voluntary compliance with the city's by-laws, checking in with local businesses to address concerns and reporting public disturbances and other issues to the Waterloo Regional Police Service (the police).

---

[13] Also, see *Cash Converters Canada Inc. v Oshawa* (*City*) 2007 ONCA 502 at para.40.
[14] Pages 6 through 10 of the Guidelines
[15] https://www.cambridge.ca/en/your-city/resources/Booklet-Ambassador-2019-8.5x8.5-WEBSITE-VERSION.pdf

[37] Also as less intrusive means, within the Core Areas, the Staff Report advises that the city installed new LED street lights with brighter directed light on certain streets, partnered with the police to ensure bike and foot patrols continue and is working with the three Cambridge business improvement areas to ensure a safe downtown environment.

[38] The city explained that the Ambassador Program and foot patrols have not been as effective as video surveillance because they do not operate 24 hours a day and are limited in size. Further, the city explained that, based on the opinion of the police, these means are less effective than video surveillance.

[39] Regarding the benefits of video surveillance, the city explained that the cameras provide passive surveillance of public areas and permit the police to officially request video recordings through its Clerk's department for specific investigations.

[40] With respect to the sensitivity of personal information, the Guidelines recommend that institutions consider the nature of the space under observation and the "closeness" of the surveillance. The city advised that it considered this and, as a result, all of the cameras are static and have no motorized zoom function.[16]

[41] As to the amount of personal information being collected, the Guidelines recommend that institutions apply the principle of data minimization. This principle entails limiting the amount of information collected to that which is necessary to fulfill the purposes of the lawfully authorized activity.

[42] In accordance with the data minimization principle, the city explained that all the cameras are:

- stationary and point at public areas;
- located on property owned by the city or region;
- restricted to prohibit the viewing of locations not intended to be monitored; and
- prevented from looking through window of an adjacent building or areas where a higher level of privacy is expected.

[43] The city also advised that the surveillance system does not have audio capabilities or the ability to collect other sensory information.

[44] At issue is whether the city has demonstrated that the collection of personal

---

[16] The city advised that the cameras have a limited zoom function, but this must be conducted manually, that is, opening the camera cover and manually zoom the lens while focusing.

information by its video surveillance system is "necessary" and not merely helpful to the proper administration of its operation of the Core Areas. To determine whether the city has shown this, Privacy Complaint Reports MC13-46 and MC13-60 are informative.

[45] In Report MC13-46, Investigator Jeffrey Cutler was not satisfied that a school board's collection of personal information through its video surveillance system was necessary to the proper administration of a lawfully authorized activity. He stated:

> I am concerned that there is no additional information to suggest that the guidelines regarding proposals for the installation of video surveillance outlined in Policy I-30 were followed by the Board prior to implementing the video surveillance system in the School. My concern in underscored by the Board's confirmation that it "… did not do a privacy impact assessment or other form of study in relation to the video surveillance program at the [S]chool." Indeed, the decision to employ video surveillance was a part of a broader initiative to implement video surveillance in all secondary schools without apparent detailed consideration to its necessity at this particular facility.
>
> Without the benefit of a privacy impact assessment, security risk assessment or similar analysis, there is no information before me to suggest that the Board considered whether less intrusive means of deterrence, such as increased monitoring by staff, were ineffective or unworkable. Similarly, there is no information indicating that the Board considered the effects of surveillance system would have on personal privacy and whether the design and operation of the video surveillance system minimizes privacy intrusion to that which is necessary, as opposed to simply helpful.
>
> In light of this, the implementation appears pre-emptive, with the only report of a security problem being thefts in the locker room (which are not covered by video surveillance in any case), and a general statement that thefts have not been more or less a problem than in previous years. Aside from this information, there is little material before me to indicate that there were demonstrative security issues at the School prior to the installation of video surveillance cameras.

[46] However, in Report MC13-60, Investigator Cutler was satisfied that a school board's collection of personal information through its video surveillance system was necessary to the proper administration of a lawfully authorized activity.

[47] He came to this conclusion based on a "'School Security Incident Matrix' that classified and listed incidents at the School prior to and after the implementation of video surveillance." Regarding this matrix, Investigator Cutler stated:

> The list is comprised of 30 specific incidents over a period of four years, although only once incident occurred after the installation of video cameras. It also identifies loitering and illegal dumping on school property as frequent and ongoing issues. The incidents included intruders in the school building or property, assaults occurring on school property, drug use, theft and vandalism. In many of the instances the Matrix indicates that a police report was filed.

[48] Because of these verifiable and specific reports of incidents, he was satisfied that the matrix demonstrated that the "safety and security events at the School are exceptional in both their severity and frequency".

[49] In this matter, the city explained that its video surveillance system is one of the measures being used to enhance public safety in its operation of the Core Areas. Further, the Staff Report advises that the city's video surveillance system "will be used to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization."[17]

[50] In my view, using a video surveillance system to help ensure the health, safety and well-being of residents, as well as to protect property, is helpful in achieving the city's safety and security objectives in the Core Areas. Moreover, based on the above, it appears that the city has considered the necessity of the collection of the personal information in accordance with the Guidelines.

[51] As described above, the city relies on police reports, the police's opinion and, the limited size and hours of operation of the Ambassador Program and foot patrols to demonstrate that the collection of personal information by its video surveillance system is necessary, and not merely helpful to the property administration of its operation of the Core Areas.

[52] Further, the city advised that, prior to operating this system, it reviewed the security camera system installed at its City Hall and outlined its video surveillance program with input from a committee composed of community, municipal and law enforcement officials.

[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:

---

[17] Section 9.2 of Schedule B to the Surveillance Policy

> 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.

[54] In this matter, the city did not provide me with any verifiable information, statistics or even specific details contained within the (police) reports of incidents that its video surveillance system will address. Moreover, the city advised that it did not conduct a privacy impact assessment, or similar analysis, before or after installing this system.

[55] Although the city advised that there is a public safety problem that is being addressed by its video surveillance system, I have nothing before me beyond its broad assertion that this problem is real, substantial or pressing, or that the less intrusive means in place are substantially less effective than this system. As a result, I find that the city has not shown that the benefits of its video surveillance system outweighs the reduction of privacy inherent in its use.

[56] For these reasons, I am not satisfied that the city has demonstrated that the collection of personal information by its video surveillance system is "necessary" and not merely helpful to the proper administration of its operation of the Core Areas.

[57] Accordingly, I am not satisfied that this collection is necessary to the proper administration of a lawfully authorized activity. Therefore, I find that the collection of the personal information by the city's video surveillance system is not in accordance with section 28(2) of the *Act*.

[58] By this finding, I am not concluding that the city's use of its video surveillance system is not necessary, per se. Rather, I conclude that the city has not demonstrated that it is necessary, or even necessary to the degree to which it has been implemented.

[59] To address this conclusion, I will recommend that the city conduct an assessment (such as, a privacy impact assessment) of its video surveillance system in accordance with the *Act*, the Surveillance Policy and this report. Doing so will help the city determine the potential, actual and type of effects that its video surveillance system may have on personal privacy. It will also help in determining the steps the city should take to mitigate those effects and minimize privacy intrusion to that which is necessary to achieve its lawful goals.

[60] Following an assessment of its video surveillance system, should the city determine that it is necessary, I recommend that the city implement the system in the Core Areas in accordance with the *Act*, the Surveillance Policy and this report.

[61] Findings regarding the city's notice of collection, use, disclosure, protection and retention of the personal information are contingent upon the valid collection of this information by its video surveillance system and, given my determination above, may not be strictly necessary at this time.

[62] However, these additional issues are before me and my findings on them will be applicable if, following an assessment(s), the city determines that its video surveillance system is necessary and implemented in a manner consistent with the *Act*, the Surveillance Policy and this report. Moreover, the results of this investigation and an analysis of the city's efforts to comply with the *Act* will be instructive to the city, stakeholders and other institutions.

[63] Therefore, as the city's video surveillance system is collecting personal information and the city may determine that it is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*, I will consider whether the city's notice of collection, use, disclosure, protection and retention of the personal information is in accordance with the *Act*.

Issue 3: Is the notice of collection in accordance with section 29(2) of the *Act*?

[64] Because the city's video surveillance system collects the personal information from individuals, generally, section 29(2) of the *Act* requires that they receive notice of the collection. This section states:

> If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

[65] To give individuals notice, the Guidelines suggest that institutions make the notice required by section 29(2) available and easily accessible on their website. The Guidelines also recommend that, at the perimeter of the monitored areas and at key locations within these areas, institutions place signs with a clear, language-neutral graphical depiction of the use of a video surveillance that also contain basic information

clarifying that video surveillance is being used.[18]

[66] In this matter, the Surveillance Policy containing the notice required by section 29(2) is available and accessible online.[19] Further, it provides that "written notice, in easily readable lettering, will be posted in the public area in a position easily viewed by the public" and that signs will have a clear, language neutral graphical depiction of the use of video surveillance and state:

> To promote safety this area is under video surveillance.
>
> Images may be recorded and/or monitored.
>
> Information collected by the use of video equipment in this area is collected under the authority of the Municipal Act, 2001 in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act.
>
> Any questions about this collection can be obtained by contacting City Clerk's Office at 519-740-4680 ext 4583.[20]

[67] As previously mentioned, the city advised that it has placed the signs described in the Surveillance Policy at the public access points to and within areas under surveillance.

[68] Based on the above, I am satisfied that the city has provided the notice required by section 29(2) and, therefore, I find that the notice of collection of the personal information is in accordance with this section.

Issue 4: Is the use of the personal information in accordance with section 31 of the *Act*?

[69] Section 31 of the *Act*, generally, prohibits the city's use of the personal information collected by its video surveillance system unless one of the exceptions under this section applies.

[70] Section 31 states:

> An institution shall not use personal information in its custody or under its control except,

---

[18] This recommendation assumes that a high percentage of the individuals whose personal information is being collected are able to read the signs (that is, are not visually disabled).
[19] https://www.cambridge.ca/en/your-city/resources/Policies---Video-Surveillance-System.pdf
[20] Sections 2.1 and 10.1 of Schedule B to the Surveillance Policy

> (a) if the person to whom the information relates has identified that information in particular and consented to its use;
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
>
> (c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the *Freedom of Information and Protection of Privacy Act*.

[71] Further, with respect to the use of personal information in the context of video surveillance, the Guidelines provide the following explanation:

> In the context of video surveillance, this means that as a general rule, institutions may only use personal information collected by means of video surveillance for the purpose of the video surveillance program or for a consistent purpose. Use of the information for other, unrelated purposes would not generally be permitted. When information collected for one purpose is used for another, unrelated purpose this is often called 'function creep.'

[72] In this matter, in my view, section 31(b) of the *Act* sets out the most applicable exception that would allow the city to use the personal information. To see whether this section applies, first, the purpose for which the personal information was obtained or compiled must be determined, and, second, whether the use of this information has taken place for either the same purpose or a consistent purpose must be determined.

[73] As previously mentioned, the city advised that the purpose for which it is obtaining or compiling the personal information is "to ensure the safety of the residents and visitors; deter unsafe activities; deter loitering on municipal streets and around public buildings; and contribute to the Cambridge Core Area revitalization."

[74] Regarding the use of the collected information, the Surveillance Policy states:

> Use of video recordings – the information collected through video surveillance is used only for the purposes of contributing to the safe environment of the Cambridge Core Area, deterring unsafe activities and assisting as one of the components of Cambridge Core Area revitalization.

[75] Based on the above, I am satisfied that the personal information collected by the city is used for the same purpose for which it was obtained or compiled.

[76] Accordingly, I find that the city's use of the personal information is in accordance with section 31(b) of the *Act* and, therefore, I find that the use of the personal information is in accordance with section 31 of the *Act*.

Issue 5: Is the disclosure of the personal information in accordance with section 32 of the *Act*?

[77] According to the Surveillance Policy, the city discloses the personal information collected by its video surveillance system as follows:

> The City of Cambridge does not disclose a video record to any individual or organization except as permitted through MFIPPA.
>
> 1. Public requests for disclosure – Any person may make a written request for access to video records created through a video surveillance system through the freedom of information process. Access may depend on whether there is a justified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record. (through appropriate request form)
>
> 2. Internal requests for disclosure – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their duties in the discharge of the corporation's function.
>
> 3. Law enforcement requests – The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system in accordance with section 32(g) of MFFIPA (through appropriate request form).

[78] The Surveillance Policy also states:

> The Freedom of Information Co-ordinator (or designate) is permitted to release copies of the records to a law enforcement agency in response to a verbal request only in situations involving an emergency, imminent danger or hot pursuit. All other requests for access by law enforcement authorities must be documented through the access request documentation utilized routinely by the Freedom of Information Co-ordinator.[21]

[79] Further, the Surveillance Policy provides that "recordings must be released if they are subject to a subpoena, search warrant, summons or other order of the courts or a quasi-judicial tribunal."[22]

[80] Section 32 of the *Act* prohibits the disclosure of the personal information by the

---

[21] Section 6.4 of Schedule B to the Surveillance Policy
[22] Section 7.2 of Schedule B of the Surveillance Policy

city unless one of the exceptions described in paragraphs (a) to (l) under this section applies.

[81] Section 32, in part, states:

> An institution shall not disclose personal information in its custody or under its control except,
>
> (a) in accordance with Part I;
>
> …
>
> (d) if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions.
>
> …
>
> (g) if disclosure is to an institution or a law enforcement[23] agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
>
> (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;

Section 32(a)

[82] The Surveillance Policy provides that the city may disclose the personal information in response to a written access request made through the freedom of information process. In my view, the exception set out in section 32(a) of the *Act* would apply to this type of disclosure.

[83] Section 32(a) allows the disclosure of personal information in accordance with Part I of the *Act*, which governs freedom of information and access to records in the custody or control of institutions.

[84] Therefore, disclosure of the personal information in response to an access request that is done in accordance with Part I would be a permitted disclosure under

---

[23] "Law enforcement" is defined in section 2(1) of the *Act* as (a) policing, (b) 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, or (c) the conduct of proceedings referred to in clause (b).

section 32(a).

[85] Accordingly, I find that the city's disclosure of the personal information in response to written public access requests made under the freedom of information process, that is, the *Act*, would be in accordance with section 32(a).

Section 32(d)

[86] The Surveillance Policy provides that the city may disclose the personal information in response to internal requests. In my view, the exception set out in section 32(d) of the *Act* would apply to this type of disclosure.

[87] Previous decisions by this office have identified the following three conditions that must be met for section 32(d) to apply:

1. The disclosure must be made to an officer, employee, consultant or agent;

2. Who needs the information in the performance of their duties; and

3. The disclosure must be necessary and proper in the performance of the institution's functions which includes the administration of statutory programs and activities necessary to the overall operation of the institution. [24]

[88] Section 32(d) makes it clear that a disclosure of personal information even within an institution must be justified and will be subject to scrutiny on a "need to know basis." The sharing of information pursuant to this section must be based on more than "mere interest or concern".[25]

[89] As indicated above, the Surveillance Policy provides that the personal information may be disclosed to an employee or consultant "if it is necessary for the performance of their duties in the discharge of the [city's] function."

[90] For this reason, I am satisfied that the conditions required for section 32(d) to apply have been met.

[91] Therefore, I find that the city's disclosure of the personal information in response to an internal request would be in accordance with section 32(d).

Section 32(g)

[92] The Surveillance Policy provides that the city may disclose the personal

---

[24] Privacy Complaint Reports MC11-73 and MC-050034-1, Investigation Reports I95-007M and I96-113P and Order PO- 1998

[25] See *H. (J.) v. Hastings* (*County*) (1993), 12 M.P.L.R. (2d) 40 (Ont. Ct. Gen. Div.)

information in response to requests from law enforcement agencies in accordance with section 32(g) of the *Act*.

[93] Specifically, this policy advises that such disclosure would occur "where there are reasonable grounds to believe that an unlawful activity has occurred and has been captured by the video surveillance system" or where the information is "subject to subpoena, search warrant, summon or other order of the courts or a quasi-judicial tribunal."

[94] Based on these conditions under which the city would disclose the personal information to a law enforcement agency, in my view, such disclosure would be an aid "to an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result."

[95] Therefore, I find that the city's disclosure of the personal information in response to a request from a law enforcement agency would be in accordance with section 32(g).

Section 32(h)

[96] The Surveillance Policy provides that the city may disclose the personal information to a law enforcement agency "in response to a verbal request only in situations involving an emergency, imminent danger or hot pursuit." In my view, the exception set out in section 32(h) of the *Act* would apply to this type of disclosure.

[97] Based on the purposes for which the city uses the personal information, that is, safety and security, in my view, it is reasonably foreseeable that "in situations involving an emergency, imminent danger or hot pursuit", these uses might require the disclosure of the personal information in such "compelling circumstances affecting the health or safety of an individual."

[98] Therefore, I find that the city's disclosure of the personal information in response to a verbal request from a law enforcement agency in the specified situations would be in accordance with section 32(h).

[99] As I have found that the circumstances in which the city may disclose the personal information are in accordance with sections 32(a),(d), (g) or (h), I find, therefore, that the disclosure of the personal information is in accordance with section 32 of the *Act*.

Issue 6: Is there a right of access to the personal information in accordance with section 36(1) of the *Act*?

[100] Section 36(1) of the *Act* gives individuals a right of access to their personal information collected by the city's video surveillance system. This section states:

> Every individual has a right of access to,

> (a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and
>
> (b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

[101] Moreover, to protect personal information when responding to access requests, the Guidelines advise that an institution's "video surveillance system should include the ability to remove or redact information from the video footage to protect exempted information."

[102] As indicated above, the Surveillance Policy provides that individuals "may make a written request for access to video records created through a video surveillance system through the freedom of information process."

[103] Further, the city advised that its video surveillance system can black out or blur images and confirmed that, pursuant to section 36(1), individuals can access their personal information collected by it.

[104] For these reasons, I find that there is a right of access to the personal information in accordance with section 36(1) of the *Act*.

Issue 7: Are there reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*?

[105] Section 3(1) of Ontario Regulation 823 (O Reg 823) requires that the city "ensure that reasonable measures to prevent unauthorized access to [individuals' information] are defined, documented and put in place, taking into account the nature of the records to be protected." This requirement "applies throughout the life-cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal."[26]

[106] In Investigation Report I93-044M, then Assistant Commissioner Ann Cavoukian stated the following about the term "reasonable measures" in section 3(1) of O Reg 823:

> The determination of whether reasonable measures had been put into place hinges on the meaning of "reasonable" in section 3(1) of Regulation

[26] Privacy Complaint Report MI10-5

> 823, R.R.O. 1990, as amended. Black's Law Dictionary defines reasonable as:
>
> > Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view ... Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable.
>
> Thus, for reasonable measures to have been put into place would not have required a standard so high as to necessitate that every possible measure be pursued to prevent unauthorized access. In our view, the measures identified above are consistent with Black's definition of "reasonable" -- appearing to be fair and suitable under the circumstances.

[107] Moreover, in Privacy Complaint Report PR16-40, then Investigator Lucy Costa stated the following about section 4(1) of Regulation 460 (which is the provincial access/privacy law equivalent of section 3(1) of O Reg 823):

> From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.

[108] Regarding video surveillance, generally, security measures should include:

- administrative measures, such as the development of clear policies and procedures regarding use and disclosure;
- technical measures, such as ensuring that images are encrypted and that robust controls are in place that ensure only those who need the information can access it (this includes logging and auditing); and
- physical measures, such as ensuring secure locations for video monitors and image storage.[27]

---

[27] Page 3 of the IPC Fact Sheet: Video Surveillance available at: https://www.ipc.on.ca/wp-content/uploads/2016/11/2016-00-09-video-surveillance.pdf

[109] Further, the Guidelines advise that, "in the context of video surveillance, security involves ensuring the confidentiality, integrity and availability of the footage captured by the system." To that end, the Guidelines set out measures that institutions may take.[28]

[110] The city provided this office with relevant information regarding the security measures in place for its video surveillance system. Some of these details are not set out in this report because disclosing them might compromise the effectiveness of these measures.

[111] Regarding administrative measures, in addition to the Surveillance Policy, the city also has a "Code of Conduct For the Employees of the City Of Cambridge" and a "City of Cambridge Privacy Policy".[29] These documents set out relevant procedures concerning the use and disclosure of the personal information collected by the city's video surveillance system and inform city employees that this information must be protected, not inappropriately accessed and handled in accordance with the *Act.*

[112] Further, the city advised that it holds privacy workshops and training for staff who access its video surveillance system and that they are required to sign a confidentiality agreement.

[113] Regarding technical measures, the city advised that video footage is encrypted and access to it is password protected. The city also advised that it would provide individuals who are able to view the footage with an auditable unique login to its video surveillance system.

[114] In addition, the Surveillance Policy specifies that the monitor can only be viewed by the city's Director of Economic Development (or designate), Manager of Technology and Support Services, and Corporate Property Manager.[30] This policy also specifies that only these individuals and the city's Freedom of Information Co-ordinator (or their designate) can view recorded footage, which "must be conducted in private and in the presence of authorized persons only", or access it."[31] Moreover, if required, access to recorded footage by the city's Technology Services staff "is limited to ensuring the system functions according to specifications."[32]

[115] With respect to live viewing of footage, the Surveillance Policy states:

---

[28] Page 17 of the Guidelines
[29] https://www.cambridge.ca/en/your-city/resources/Code-of-Conduct-for-the-Employees.pdf and https://www.cambridge.ca/en/your-city/resources/Privacy-Policy---June-2014.pdf
[30] Section 4.1 of Schedule B of the Surveillance Policy
[31] Sections 6.3 and 6.5 of Schedule B to the Surveillance Policy
[32] Sections 5.2, 6.3 and 6.5 of Schedule B to the Surveillance Policy

> Live viewing is restricted to time periods when there is higher likelihood of safety and security concerns, or the commission of unauthorized activity in the area under surveillance Live feed monitors are turned off when not in use.

[116] When disclosing personal information in accordance with the *Act*, the Guidelines advise that "it is important that disclosures be done in a manner that protects the privacy and security of the personal information." To that end, the Guidelines recommend that institutions maintain an auditable log of each disclosure and ensure that this log contains certain information.

[117] The Surveillance Policy requires that "requests for access [to video footage] by law enforcement authorities must be documented through the access request documentation utilized routinely by the FOI co-ordinator."[33] In addition, it provides that access to video footage will be logged as follows:

> A log will be kept to record access to the recordings. An entry will be made each time the recordings are consulted or any time a copy if made of any part of them. The log entry will note the person(s) accessing the recordings and the reason for access.[34]

[118] Based on my review of the logs used by the city when it discloses the personal information collected by its video surveillance system, generally, I am satisfied that these forms contain the information recommended by the Guidelines.[35]

[119] With respect to system review and audits, the Guidelines recommend that institutions regularly audit the roles, responsibilities and practices of its video surveillance program regularly to ensure that they comply with its policies and procedures.

[120] To this end, the city advised that it audits the logs annually and that its staff can perform random audits. Further, the city advised that its policies must be reviewed in 2024 and that its video surveillance system is checked once a year to ensure that all of the cameras are pointed correctly and are operating sufficiently.

[121] Regarding physical measures, according to the Surveillance Policy, "the recording and storage equipment will be stored in a secure, non-public area at all times" and that "one secure monitor is located in the Office of the Corporate Property Manager."[36] The city also advised that it would restrict devices capable of recording (for example, cell

---

[33] Section 6.4 of Schedule B to the Surveillance Policy
[34] Section 7.1 of Schedule B to the Surveillance Policy
[35] Pages 14 to 15 in the Guidelines
[36] Sections 4.1 and 6.1 of Schedule B to the Surveillance Policy

phones) from this manager's office.

[122] Based on the above, I am satisfied that the city has put in place reasonable measures to safeguard the footage collected by its video surveillance system. Therefore, I find that there are reasonable measures in place to protect the personal information as required by section 3(1) of O Reg 823 under the *Act*.

Issue 8: Does the city have proper retention periods in place for the personal information?

[123] Section 30(1) of the *Act* requires that the city keep the personal information collected by its video surveillance system "for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information."

[124] To that end, section 5 of O Reg 823 prescribes the following period:

> An institution that uses personal information shall retain it for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, except if,
>
> (a) the individual to whom the information relates consents to its earlier disposal; or
>
> (b) the information is credit or debit card payment data.

[125] Together, section 30(1) and section 5 of O Reg 823 establish a default minimum one-year retention period for used personal information,[37] subject to the exceptions set out in section 5 of O Reg 823.

Used Video Footage

[126] Where video footage has been used, it would be subject to the one-year minimum retention period indicated above. The Guidelines advise that, "in the context of video surveillance, personal information is used whenever footage that contains images of individuals or other identifiable information is accessed or disclosed." It also advises that, "simply viewing a live feed does not represent a 'use' of personal information".

[127] Regarding used video footage, the Surveillance Policy states:

---

[37] Privacy Complaint Reports MC10-2, MC13-46, MC13-60 and MC17-32

> In cases where the surveillance system records activities that relate to an insurance, liability, law enforcement or other similar issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time.[38]

[128] For this reason, I am satisfied the city's retention period for used personal information is in accordance with the minimum one-year retention period.

[129] Therefore, I find that the retention of used personal information is in accordance with section 30(1) of the *Act*.

Unused Video Footage

[130] Where video footage has not been used, the Guidelines recommend that its retention period be limited as follows:

> Recorded information that has not been used is routinely erased according to a standard schedule. Under the standard schedule, the retention period for unused information is limited to the amount of time reasonably necessary to discover or report an incident that occurred in the space under surveillance.[39]

[131] The Guidelines also advise that "when erasing or deleting recorded information, whether used or unused, it is critical that the information and old storage devices are disposed of in such a way that the personal information cannot be reconstructed or retrieved."[40]

[132] The city advised that unused video footage is retained until its system's electronic storage capacity is reached or up to 30 days, whichever comes first. Once capacity is reached or 30 days have passed, the city explained that the unused footage is permanently erased, that is, overwritten. The city further explained that it chose a (maximum) 30-day schedule based on the opinions of both the provider of its video surveillance system and the police.

[133] I am satisfied that the city has provided a reasonable basis after consultation with the video surveillance system provider and the police for retaining the unused video footage for this period.

[134] For this reason, I am satisfied that the retention of the unused personal

---

[38] Section 6.2 of Schedule B to the Surveillance Policy
[39] Page 10 of the Guidelines
[40] Page 11 of the Guidelines

information collected by the city's video surveillance system is in accordance with the *Act*.

[135] Therefore, I find that the city has proper retention periods in place for the personal information.

The city's consultation with stakeholders

[136] The *Act* does not require that institutions consult with anyone about the collection of personal information where such collection is necessary to the proper administration of a lawfully authorized activity.

[137] However, the Guidelines recommends that individuals who might be affected by video surveillance should be consulted as follows:

> The use of video surveillance affects all the individuals who end up moving within the space under observation. Therefore, prior to using video surveillance, and where feasible to do so, [an institution] should identify those who reasonably may be affected by the video surveillance and consult with them as to the program's necessity and impact.[41]

[138] The matter of consultation raises two questions. The first question is: who are the stakeholders? For this question, "context is important, and in each circumstance where the installation of cameras is considered the questions should be asked who may be reasonably affected by the video surveillance? And, is consultation feasible?[42]

[139] The second question is: were the stakeholders adequately consulted?[43] Consultation is more than merely announcing the decision to implement video surveillance.[44]

[140] The city advised that camera placement was determined with input from the police and the Downtown Cambridge Business Improvement Area based on their experience with the city's downtown activities, as well as from the Regional Municipality of Waterloo.

[141] The city also advised that a committee of community, municipal and law enforcement stakeholders came together to outline the video surveillance program. Further, the Staff Report lists various internal and external stakeholders that the city consulted regarding its video surveillance program.

---

[41] Page 19 of the Guidelines
[42] Privacy Complaint Report MC13-60.
[43] Privacy Complaint Report MC13-60.
[44] Privacy Complaint Reports MC13-60 and MC13-67.

[142] Moreover, as previously indicated, the city's council approved the Surveillance Policy before any of the video surveillance cameras began recording.

[143] In light of the aforementioned steps taken, I commend the city for its consultations with stakeholders regarding the implementation of its video surveillance system.

CONCLUSION:

Based on the results of my investigation, I have reached the following conclusions:

1. The information at issue is "personal information" as defined by section 2(1) of the *Act*.

2. The collection of the personal information is not in accordance with section 28(2) of the *Act*.

3. The notice of collection is in accordance with section 29(2) of the *Act*.

4. The use of the personal information is in accordance with section 31 of the *Act*.

5. The disclosure of the personal information is in accordance with section 32 of the *Act*.

6. There is a right of access to the personal information in accordance with section 36(1) of the *Act*.

7. There are reasonable measures in place to protect the personal information as required by section 3(1) of Ontario Regulation 823 under the *Act*.

8. The city has proper retention periods in place for the personal information.

9. The city properly consulted with stakeholders.

RECOMMENDATIONS:

Based on the above conclusions, I make the following recommendations:

1. I recommend that the city conduct an assessment of its video surveillance system in a manner consistent with the *Act*, the Surveillance Policy and this report, to determine whether the collection of personal information by the system is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*.

2. Following an assessment of the video surveillance system and assuming a determination by the city that it is necessary, I recommend that the city implement the system in a manner consistent with the *Act*, the Surveillance Policy and this report.

3. Within six months of receiving this report, the city should provide this office with proof of compliance with the above recommendations.

The city has reviewed this report and agreed to implement the above recommendations. Accordingly, within six months of receiving this report, the city should provide this office with proof of compliance with these recommendations.

Original Signed by: April 23, 2021

John Gayle
Investigator