Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. MC10-2

City of Mississauga

October 29, 2010

Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **MC10-2**

INVESTIGATOR: **Mark Ratner**

INSTITUTION: **City of Mississauga**

SUMMARY OF COMPLAINT:

The Office of the Information and Privacy Commissioner/Ontario (IPC) received a privacy complaint from an individual (the complainant) under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) relating to the City of Mississauga (the City).

The complainant stated that he attended at the Mississauga Civic Centre (the Civic Centre) for the purposes of filing a Freedom of Information (FOI) request under the *Act*. The complainant explained that FOI requests are filed at a counter located in the City Clerk's office. The complainant stated that at the time of filing the request, he noticed a video surveillance camera directly above the counter. The complainant expressed concern that the video surveillance camera may be used to identify himself and other individuals filing FOI requests. The complainant also made reference to surveillance cameras in City Council Chambers, which is within the Civic Centre.

In response to the complaint, the IPC commenced a privacy investigation to review the video surveillance practices of the City at the Civic Centre. As part of the investigation, the IPC Investigator conducted a site visit.

Background Information

In response to the complaint, the City provided detailed information concerning the video surveillance system (the system) in operation at the Civic Centre. The City also provided our office with a copy of its Corporate Policy and Procedure on video surveillance (the Policy), as well as background documentation. As noted above, the IPC conducted a site visit of the Civic Centre to examine the video surveillance system.

The City advised that there are currently 63 cameras located within the Civic Centre. Cameras are located in the Civic Centre parking lot, the fitness centre, the Council Chambers, the Clerk's office area, and in other areas within the building.

The City has provided the IPC with additional relevant information regarding the system and the security measures in place. Some of the details of the system and the security measures in place are not set out in this report because disclosure might compromise the effectiveness of the security measures.

The City indicated that it has a total of 19 signs located throughout the Civic Centre informing the public that video surveillance is in effect.

DISCUSSION:

In what follows, I address whether the City's video surveillance system accords with the privacy protection rules set out in the *Act*. Among other things, the *Act* sets out rules relating to the collection, notice, use, disclosure, security, and retention of personal information. In conducting this analysis, I will make reference to the IPC's *Guidelines for the Use of Video Surveillance Cameras in Public Places*[1] (the *Guidelines*). The IPC's *Guidelines*, which were originally published in 2001 and were updated in 2007, set out best practices for institutions to follow when implementing video surveillance programs.

The following issues were identified as arising from the investigation:

Is the information "personal information" as defined in section 2(1) of the *Act*?

The information in question is the recorded images collected through the video surveillance cameras that are located in the Civic Centre.

Section 2(1) of the *Act* states, in part:

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

The IPC has previously held that information collected about identifiable individuals from video surveillance cameras qualifies as "personal information" under the *Act* [see *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, MC07-68]. In this case, the City has taken the position that the information collected from the video surveillance cameras qualifies as "personal information" under the *Act*.

[1] http://www.ipc.on.ca/images/Resources/video-e.pdf .

Based on the above, I concur that the images of identifiable individuals collected from video surveillance cameras located within the Civic Centre qualify as "personal information" under section 2(1) of the *Act*.

Was the collection of the "personal information" in accordance with section 28(2) of the *Act*?

Section 28(2) of the *Act* 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.

This provision sets out the circumstances under which personal information may be collected by an institution. In order for such a collection to be permissible, it must satisfy one of the following conditions: it must either be (a) authorized by statute, (b) used for purposes of law enforcement, or (c) necessary to the proper administration of a lawfully authorized activity.

In this case, the City has stated that the personal information is collected both for the purposes of law enforcement and because it is necessary to the proper administration of a lawfully authorized activity.

I will first consider whether the collection is necessary to the proper administration of a lawfully authorized activity. In order to make this determination, the City must first show that the activity is **lawfully authorized**, and second, that the collection of the personal information is **necessary** to that lawfully authorized activity.

The City's operation of the Civic Centre is lawfully authorized by virtue of section 11(1) of the *Municipal Act, 2001*, which 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 … .

The activity in question is the operation of the Civic Centre, which the City deems to be "necessary or desirable" for the public. I am satisfied that the operation of a municipal building is a lawfully authorized activity.

The City has also stated that the collection of images through the video surveillance program is necessary to the operation of the Civic Centre: it is required to support the proper allocation and administration of staff duties, to ensure the safety of both staff and the public, and to provide for the protection of City assets.

I have considered the explanation provided by the City. I acknowledge that the presence of security cameras in buildings is recognized as being beneficial to the security of people and property. Accordingly, in the circumstances of this case, I am satisfied that the collection of

personal information through video surveillance is necessary to the proper administration of the Civic Centre, which is a lawfully authorized activity. The collection of personal information is in accordance with section 28(2) of the *Act*.

Because of my conclusion above, it is not necessary for me to consider whether the collection of the personal information is permissible for the purposes of law enforcement.

Did the City provide Notice of Collection as required under section 29(1) of the *Act*?

Section 29(1) of the *Act* imposes a Notice requirement on institutions that collect personal information, and 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.

The *Guidelines* elaborate on the Notice requirements as follows:

> The public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance area … so that the public has reasonable and adequate warning that surveillance is or may be in operation … .
>
> [N]otification requirements under … section 29(2) of the *Act* include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of someone who can answer questions about the collection. This information can be provided at the location on signage and/or by other means of public notification such as pamphlets or the organization's website. …

In sum, the *Guidelines* state that notice of the video surveillance should be given through signs placed at the site. The full notice requirement prescribed under the *Act* (which includes the legal authority for collection, a statement of the principal purposes of the collection, and contact information) may be satisfied through a combination of signs and other forms of notice, such as pamphlets or the internet.

The City advised that there are currently 19 signs in place in the Civic Centre. The signs state that "these premises are monitored by Automated Video Surveillance" and provide contact information for the Manager of Security and Operations for any questions regarding the surveillance program. The IPC Investigator observed these signs during the site visit to the Civic Centre.

The City has also posted a Notice on its website[2], which states, in part:

> The personal information collected by the use of the City's video surveillance cameras is collected under the authority of the *Municipal Act*, Section 11 and the City's Corporate Policy on Video Surveillance. The information is used for the purpose of promoting public safety, aiding the risk management insurance program and reducing crime at City facilities.
>
> Any questions about this collection can be directed to the Access and Privacy Officer, Corporate Services Department, Office of the City Clerk … .

The City has provided the IPC with a copy of a pamphlet that contains wording similar to that appearing on the City's website.

Having reviewed all the various forms of notice provided by the City, I am satisfied that it is satisfying the notice requirements set out in section 29(2) of the *Act*, and the IPC's *Guidelines*.

Is the City's use of the information obtained from the video surveillance cameras in accordance with section 32 of the *Act*?

The City's Policy outlines the various uses of the personal information obtained through its video surveillance program as follows:

> The information collected through video surveillance is used only:
>
> - to assess the effectiveness of safety and security measures taken at a particular Facility;
> - to investigate an incident involving the safety or security of people, facilities, or assets;
> - to provide law enforcement agencies with evidence related to an incident under police investigation;
> - to provide evidence as required to protect the City's legal rights;
> - to respond to a request for information under the *Municipal Freedom of Information and Protection of Privacy Act*;
> - to investigate an incident or allegation of serious employee misconduct; or

[2] http://www.mississauga.ca/portal/residents/civicfacilities?paf_gear_id=9700018&itemId=103300439n&returnUrl=%2Fportal%2Fresidents%2Fcivicfacilities .

- to investigate an incident involving an insurance claim.

In my view, two of the items listed above are more properly characterized as "disclosures" rather than "uses": (1) to provide evidence to law enforcement agencies, and (2) to respond to a request for access to information under the *Act*. Accordingly, these two items will be addressed below, under the section dealing with the disclosure of personal information.

In order to determine whether the remaining uses identified by the City accord with the *Act*, it is necessary to consider section 31 of the *Act*, which states:

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

Section 31 prohibits the use of personal information, subject to the three statutory exceptions listed above. In order for a given use of personal information to be permitted under the *Act*, it must satisfy at least one of the exceptions.

In this case, the exception that is most applicable to the present circumstance is section 31(b), which permits the use of personal information for the purposes for which it was obtained or compiled, or for a consistent purpose. In order to determine whether this exception applies, it is necessary to first consider the purpose for which the records were obtained or compiled, and then determine whether the use has taken place for either the same purpose or a purpose that is consistent with the original purpose of the collection.

As noted above, the City has stated that the information is collected to support staff duties, to protect the safety of staff and the public, and for the protection of City assets. All of these purposes relate to the proper administration of a municipal building.

The uses of personal information listed above relate to safety, conduct of employees, and the investigation of insurance claims. In my view, these uses are all elements of the proper administration of a municipal building, which is the original purpose of the collection.

Accordingly, I am satisfied that the personal information obtained from the City's video surveillance program is used for the same purpose for which it was originally obtained or compiled, namely, the administration of a municipal building, and accords with the permitted use in section 31(b) of the *Act*.

Whether the City's disclosure of the personal information obtained from the video surveillance system is in accordance with section 32 of the *Act*?

The City's Policy listed two potential disclosures of personal information from the video surveillance program: (1) disclosure to law enforcement agencies in relation to an investigation; and (2) disclosure in response to a request for access under the *Act*.

Section 32 of the *Act* states:

> An institution shall not disclose personal information in its custody or under its control except,
>
> (a) in accordance with Part I;
>
> (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
>
> (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> …
>
> (g) if disclosure is to an institution or a law enforcement 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;
>
> … .

Section 32 contains a general prohibition on the disclosure of personal information subject to a series of exceptions. I will address each of the two potential disclosures of personal information.

I will first address the potential disclosure of personal information to a law enforcement agency. The City has provided an example of a situation where such a disclosure may occur. The City explained that the police sometimes investigate thefts from cars parked in the Civic Centre parking garage. In such cases, information obtained from a video surveillance camera would be provided to the police to assist in their investigation into the theft.

Section 32(g) permits the disclosure of personal information to a law enforcement agency to aid in an investigation from which a law enforcement proceeding is likely to result. I note that the type of disclosure described by the City (e.g., thefts from the parking garage) would qualify as a disclosure to "aid in an investigation from which a law enforcement proceeding is likely to result."

I am therefore satisfied that the disclosure by the City of personal information from the video surveillance program to a law enforcement agency constitutes a permissible disclosure under section 32(g) of the *Act*.

The second type of disclosure contemplated by the City's Policy is the disclosure of records in response to a request for access under Part I of the *Act*.

Section 32(a) of the *Act* permits the disclosure of personal information in "accordance with Part I" of the *Act*, which establishes rules relating to access to records in the custody or control of government institutions. Accordingly, a disclosure in response to a request for access to records would constitute a permitted disclosure under section 32(a), subject to the appropriate mandatory and discretionary exemptions that may apply to the records.

Based on all of the above, I am satisfied that the disclosures of personal information that are contemplated and undertaken by the City are in accordance with section 32 of the *Act*.

Has the City implemented adequate measures to protect the security of the personal information as required under section 3(1) of Ontario Regulation 823, made pursuant to the *Act*?

Section 3(1) of Ontario Regulation 823, made pursuant to the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

This provision mandates that institutions take reasonable measures to prevent unauthorized access to records in their custody. The *Guidelines* elaborate on this requirement by outlining the security measures that an institution should take to protect video surveillance records in their custody and control. The *Guidelines* recommend the following measures:

- that video images be stored in a locked receptacle in a controlled access area;
- access to video images be limited to authorized personnel, and that logs of access should be maintained for audit purposes;
- written polices should state who should be able to view records and for what purpose;
- that staff be trained on their obligations under the *Act*;
- employees of institutions and service providers sign written agreements regarding the system; and
- the video surveillance system should be subject to regular reviews and audits.

I have reviewed the information provided by the City, including its Policy in order to determine whether the security measures in place are reasonable under section 3(1) of Ontario Regulation 823, and accord with the recommended measures set out in the IPC's *Guidelines*.

With respect to the requirement that images be stored in a locked receptacle in a controlled access area, the City has stated that it has provided for the safe and secure storage of images, and particulars of this storage have been provided to this office.

During the site visit, the IPC observed and confirmed that the DVRs were located in areas where access was controlled by card readers.

With respect to access to images taken from the video surveillance system, the City's Policy states that an access request form must be filled out and provided to the City's Manager of Security before access is permitted. Further, the Policy states that whenever access is given, the following must be logged for audit purposes:

- the date and time at which the access was allowed or the date on which disclosure was made;
- the identification of the party who was allowed access or to whom disclosure was made;
- the reason for allowing access or disclosure;
- the extent of the information to which access was allowed or which was disclosed; and
- provisions for the return of the record or its destruction.

Requests for access to records are provided to a senior member of Security staff, who, upon receiving a completed request form, isolates the digital images that are the subject of the request, and transfers the images to a DVD. The senior member of Security staff can only access the system through a password.

The Policy also includes a requirement that all system operators are trained properly on the use of the video surveillance system, and that anyone having access to records created by the system is "required to sign a written agreement regarding his or her duties, obligations, and responsibilities with respect to the use and disclosure of the record."

With respect to system reviews and audits, the City has stated that the Manager of Security conducts an annual review of all security systems within the Civic Centre, which includes the video surveillance program.

Based on the above, I am satisfied that the City has met its obligations under section 3(1) of Regulation 823 under the *Act*.

Has the City implemented retention policies that accord with section 5 of Ontario Regulation 823, made pursuant to the *Act*, as well as the *Guidelines*?

Section 5 of Ontario Regulation 823 sets out the retention requirements for records of personal information in the custody or control of an institution and states:

> Personal information that has been used by an institution shall be retained by the institution 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, unless the individual to whom the information relates consents to its earlier disposal.

This provision establishes a minimum 1 year retention period (or less when set out in a by-law or other resolution of the institution) for video surveillance images that have been used.

The *Guidelines* address retention and draw a distinction between records that have been used (*i.e.*, viewed for a law enforcement or public safety purpose) and video surveillance records that have not been used. In cases where images have been accessed and viewed, they would be subject to the 1 year retention requirement set out above. In cases where images have not been used, the *Guidelines* state:

> Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule (normally between 48 and 72 hours). For example, images are not monitored from a video surveillance system in Toronto's entertainment district introduced in 2007. Images are overridden automatically every 72 hours and are not accessed unless an incident prompts an investigation.

With respect to the City's video surveillance program, the City has stated that where video surveillance images are used for an investigation, the images are "retained on a DVD for 7 years."

In cases where images are not used for the purposes of an investigation, images "are retained electronically on the DVR hard drives and are overwritten on a 'first in, first out' basis." The length of time such images are retained in DVRs varies from 21 to 90 days, depending on the capacity of the DVR in question.

The City explained that the retention periods differ in length because of the differing capacities of the hard drives of the seven DVRs. Once a DVR has reached full capacity, it will overwrite the oldest recording on a first-in, first out basis.

The City has also explained its rationale for maintaining records images for more than the 72 hours recommended by the *Guidelines*. The City has stated that it is often required to investigate incidents that are reported weeks after they occur. The City has noted that it co-operates with the Police in investigating certain incidents, and the Police sometimes do not request copies of images until more than 72 hours after an incident has occurred.

In the City's view, having the DVRs overwrite on a 72 hour retention schedule would entail that these records would not be available for investigative purposes.

I have considered the information provided by the City and I am satisfied, that in the circumstances of this case, the City has demonstrated its necessity to maintain images for longer than the 72 hour retention period recommended by the *Guidelines*.

As a result of this investigation, the City has agreed to a standardized retention period.

Do the cameras in the City Clerk's office capture the identity of individuals filing FOI requests?

The complainant's complaint expressed concern that his identity as an FOI requester may be revealed as a result of the video surveillance cameras present in the City Clerk's office.

During the site visit, the IPC Investigator observed that one of the cameras in the Clerk's office was positioned so that it could record the images of individuals filing FOI requests.

The City advised that the camera in question was intended to be fixed on point of sale equipment in the Clerk's office, and was not intended to capture the images of individuals filing FOI requests. The City also stated that the camera was not used to identify individuals filing FOI requests. The City further explained that other City business is conducted at the counter where FOI requests are filed, and accordingly, appearance at the counter does not identify an individual as an FOI applicant.

The City stated:

> Once it came to our attention that the camera could in fact identify individuals filing MFIPPA requests, the City immediately had the camera repositioned to satisfy the original intent.

In response to this complaint and investigation, the City re-positioned the camera in question in the Clerk's office so that it could no longer capture the images of individuals filing FOI requests in person. The City also stated that the camera did not have pan-tilt-zoom capabilities.

Based on the information provided by the City and gathered during the site visit, I am satisfied that while the camera in question had originally been positioned in a manner that captured images of individuals filing FOI requests, the intended use for this camera was not this purpose, and the camera has since been repositioned.

CONCLUSION:

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

1. Information collected through the video surveillance system qualifies as "personal information" under section 2(1) of the *Act*.

2. The collection of the personal information is in accordance with section 28(2) of the *Act*.

3. The City has provided Notice of Collection in accordance with section 29(2) of the *Act*, and the IPC's *Guidelines*.

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

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

6. The City has implemented reasonable measures to protect the security of personal information as required under section 3(1) of Ontario Regulation 823.

7. The City's retention periods accord with section 5 of Ontario Regulation 823, as well as the *Guidelines*.

8. The camera located in the office of the City Clerk is not used to identify individuals filing FOI requests.

October 29, 2010

Mark Ratner
Investigator