

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 MC13-60

Toronto Catholic District School Board

July 17, 2015

Summary: The complainant, whose residence is adjacent to the Monsignor Fraser College (the School) in Toronto, expressed concern with the use of video surveillance at the School, which is operated by the Toronto Catholic District School Board (the Board). The Information and Privacy Commissioner/Ontario (the IPC) finds that the Board's collection of the personal information within the School property is in accordance with section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). However, the collection of personal information from outside the School's property is not in accordance with section 28(2) of the *Act*.

This Report also considers whether the Board's use, disclosure, retention and security of personal information are in compliance with the *Act*.

The IPC makes recommendations regarding the collection of personal information from outside the School's property and revision of the Board's notice and policy on video surveillance.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. M.56, as amended, ss. 2, 28, 29, 31, 32 and 36; R.R.O. 1990, Reg. 823, ss. 3 and 5; *Education Act* R.S.O. 1990, c. E.2, ss. 170 and 265; R.R.O. 1990, Reg. 298, s. 11.

Orders and Investigation Reports Considered: MC07-68; MC10-2; MC13-46.

BACKGROUND:

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 Toronto Catholic District School Board (the Board).

The complainant's residence is adjacent to the Monsignor Fraser College (the School) campus located at 700 Markham Street, Toronto. The complainant became aware of external video cameras installed at the School and is concerned that the video surveillance system is collecting the personal information of himself and his neighbours.

The complainant explained that he expressed his concerns to the Board, but asserts that he was informed by the Board's head of security that he was not involved in any decision about when and why video cameras were installed and was referred to the Superintendent of Facility Services. At the time of filing the complaint with the IPC, the complainant asserted that he had yet to receive a response from the Board.

The IPC commenced a privacy investigation to review the video surveillance practices of the Board at the School. As part of the investigation, the IPC Investigator conducted a site visit.

In response to the complaint, the Board provided detailed information concerning the video surveillance system in operation at the School, which has a population of approximately 150-200 students. The Board also provided our office with a copy of the relevant policy titled "Policy B.M.07". During the course of the investigation, the Board implemented a revised video surveillance policy that I will also review as part of my analysis.

The Board explained that in April 2013, 19 video cameras, comprising of 12 internal and 7 external cameras, were installed in the School.

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

Signs are located at the School entrances informing individuals that video surveillance is in effect.

DISCUSSION:

The following addresses whether the Board'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 Privacy Complaint Report MC13-46¹ and the IPC's

¹ <https://www.ipc.on.ca/images/Findings/MC13-46.pdf>.

*Guidelines for Using Video Surveillance Cameras in Schools*² (the *Guidelines*). The IPC's *Guidelines*, which were originally published as a paper in 2003 and were updated in 2009, set out best practices for institutions to follow when implementing video surveillance programs in schools.

The circumstances of this complaint are very similar to those that arose in Privacy Complaint Report MC13-46. That Report also addressed issues of notice, collection, use, retention and security as they concern the implementation of video surveillance in a secondary school. Due to the similarities, much of the findings made in this Report will mirror those that I made in Privacy Complaint Report MC13-46.

The following issues arose from the investigation.

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

In order to determine whether the Board has complied with the scheme under the *Act* for the protection of personal privacy, it is first necessary to decide whether the information is “personal information”.

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

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* and Privacy Complaint Reports MC07-68³ MC10-2⁴ and MC13-46]. The Board agrees that the information collected from the video surveillance cameras qualifies as “personal information” under the *Act*.

Based on the above, I find that the images of identifiable individuals collected from video surveillance cameras located within the School qualify as “personal information” under section 2(1) of the *Act*.

² www.ipc.on.ca/images/Resources/vidsch-e.pdf

³ http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf

⁴ www.ipc.on.ca/images/Findings/MC10-2.pdf

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.

The Board explained that the collection of personal information is necessary to the proper administration of a lawfully authorized activity. In order to make this determination, the Board 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.

I will first consider whether the circumstance in which the collection occurs is a lawfully authorized activity.

In Privacy Complaint Report MC13-46, I agreed that the Halton Catholic District School Board’s operation of a school is lawfully authorized under section 170(1) of the *Education Act*. Furthermore, I noted that “[t]he operation of the School includes responsibility for the safety and security of students and property as set out in section 265(1) of the *Education Act* and section 11(3) of Regulation 298.” The same reasoning applies in the circumstances of this complaint.

The next question to consider is whether the collection of personal information via a video surveillance system is necessary to the operation of the School. The requirement that the collection be “necessary” to the proper administration of a lawfully authorized activity means that it must be more than merely helpful:

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 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.⁵

In response to this investigation, the Board provided the “School Security Incident Matrix” that classified and listed incidents at the School both prior to and after the implementation of video surveillance in April 2013. The list is comprised of 30 specific incidents over a period of four years, although only one incident occurred after the installation of video cameras. It also

⁵ Special Investigation Report, MC07-68, at page 21: https://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf.

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.

Regarding the collection of personal information from within the School property, I am satisfied that the Board has demonstrated that the collection of personal information is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*. I base this conclusion on the information in the School's Security Matrix. The safety and security events at the School are exceptional in both their severity and frequency, and I am satisfied that the collection of personal information within the School property via the video surveillance system is necessary to the operation of the School.

However, I am not convinced that the collection of personal information from *outside* the School's property is necessary within the meaning of section 28(2). As described above, the complainant lives on property next to the School and expressed concern with the positioning of cameras such that they observe the residences and public areas outside of the School grounds.

During my site visit to the School, the Board provided me an opportunity to view the video displays for their cameras. Although the Board had employed measures to limit the capture of images outside of the School grounds, the capacity existed to view some of the neighbouring properties. From my observations, the collection of personal information of individuals outside the School grounds occurs when an operator uses the "pan-tilt-zoom" function on a camera. External cameras that are fixed in place only capture images from School property.

The Board acknowledges that it did not require or intend to include surveillance of areas outside of the School property. It did not take the position that the collection of personal information from those areas was necessary to the operation of the School.

In response to my concerns regarding the capacity to view areas outside of its property, the Board agreed to undertake measures to ensure that video surveillance did not include these areas. Subsequently, the Board provided me with samples of their revised image capture capacity. I have confirmed that the Board no longer has the capacity to capture images of the complainant's residence. However, as of the date of this Report, I am not satisfied that the School's cameras are no longer able to capture images of other areas outside of the School property. As the collection of personal information outside of the School property is not in accordance with section 28(2) of the *Act*, I shall recommend that the Board cease the collection of personal information from outside of the School property via the video surveillance system.

Did the Board provide a Notice of Collection as required under section 29(2) of the *Act*?

Section 29(2) 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* provide direction to boards concerning the Notice requirements as follows:

This provision [section 29(2)] requires that institutions inform 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. At a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact the school office with any questions. The remainder of the notice requirements under the *Acts* can be satisfied through information pamphlets available in the school office or information posted on the school board's website.

In summary, 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 also be satisfied through a combination of signs and other forms of notice, such as pamphlets or the internet.

The Board's revised Policy B.M.07 requires that notices are clearly displayed at the perimeter of the video surveillance area informing that cameras are in use. Currently, notices are located at the two main entrances to the School as well as on a side of the building in the parking lot. The placement of the existing notices is consistent with Policy B.M.07 and the *Guidelines*.

Regarding the content of the notice, the Board acknowledged that its signage does not accord with sections 29(a) and (c) of the *Act*. The existing signage states "Warning These Premises are Under 24 Hour Video Surveillance" and includes an icon of a video camera. Having reviewed the notice provided by the Board, I am not satisfied that it meets the requirements set out in section 29(2) of the *Act*. Therefore, I recommend that the Board revise its notice to include the following information:

- Video Surveillance in Use.
- This facility is monitored by 24 hour video surveillance.
- Security cameras are in operation for the safety of the students, staff and the school community and for the protection of Board property.

- The information is collected under the authority of the *Education Act* in compliance with *MFIPPA*. For additional information please contact the Principal/Manager of this site or contact the Board Office at (contact information).

Is the Board's use of the information obtained from the video surveillance cameras in accordance with section 31 of the *Act*?

Section 31 of the *Act* prohibits the use of personal information in its custody or under its control unless at least one of three exceptions is met. It 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*.

Policy B.M.07's stated purpose is to assist in providing a safe and secure environment, and directs that "[v]ideo surveillance shall not be used to monitor staff performance." There is no additional information within Policy B.M.07 describing either permissible or impermissible uses.

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.

The Board states that the uses of the personal information obtained from the video surveillance system are in accordance with section 31(b) of the *Act*. As noted above, the Board has stated that the information is collected to protect the safety of students and staff, and for the protection of Board property. The uses of personal information listed above relate to safety and security of the property. In my opinion, these uses are all elements of the proper administration of a school, which is the original purpose of the collection.

Therefore, I find the Board's use of the personal information is in accordance with section 31 of the *Act*. The personal information obtained from the video surveillance program is being used for the same purpose for which it was originally obtained or compiled, specifically, the administration of a school, and accords with the permitted use in section 31(b) of the *Act*.

Although Policy B.M.07 states that the authority of the Director to operate the video surveillance system may be delegated to principals, facility managers and other employees and is not to be used for staff performance monitoring, no other description of the limitations on use is provided. I recommend that the Board include additional information regarding the limits on its use, having regard to the *Guidelines*.

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

Policy B.M.07 identifies two potential disclosures of personal information from the video surveillance program: (1) disclosure "upon written request for the purposes of law enforcement"; and (2) disclosure in response to a request for access under the *Act*.⁶

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 now address each of the two potential disclosures of personal information identified in the Board's Policy.

Section 32(g) permits the disclosure of personal information to a law enforcement agency to aid in an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. The Board asserts the disclosure to a law enforcement agency of any information obtained through video surveillance would be in compliance with the *Act* and its own internal policies. However, Policy B.M.07 is not as specific, instead referring to

⁶ Policy B.M.07 references section 32(f) of the *Act* in regards to external requests for video surveillance footage. Section 32(f) applies to disclosures by law enforcement agencies to either domestic or foreign law enforcement agencies and is not applicable to school boards.

written requests from police in relation to law enforcement. In its submissions, the Board explained that in regards to disclosures under section 32(g), school principals work directly with law enforcement and explained that these procedures are governed by the Police-School Board Protocol.⁷

I have reviewed the Police-School Board Protocol referenced by the Board. This document includes a section on disclosures by boards to the Toronto Police Service and makes specific reference to section 32(g) of the *Act* and IPC resources. The information in the Police-School Board Protocol as it pertains to disclosures under section 32(g) is consistent with the *Act*.

I note that the type of uses of the video surveillance system as described in Policy B.M.07 (e.g., safety and security) would foreseeably entail disclosures to law enforcement. Such disclosures qualify as aids to “an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.”

I am therefore satisfied that disclosure by the Board of personal information obtained from the video surveillance system to a law enforcement agency constitutes a permissible disclosure under section 32(g) of the *Act*. That said, I suggest the Board revise its policy to mirror the wording of the *Act*, to include law enforcement, and to explain that such disclosures are in relation to investigations.

The second type of disclosure contemplated is 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 institutions. A disclosure in response to an access request 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 Board are in accordance with section 32 of the *Act*.

Whether the Board permits access to personal information obtained from the video surveillance system in accordance with section 36 of the *Act*?

Section 36(1) 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 control of an institution with respect to which the

⁷ <http://www.torontopolice.on.ca/publications/files/misc/schoolprotocol.pdf>

individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

Section 36(1) provides individuals with a general right of access to their personal information that is in the custody or control of an institution. The Board asserts that individuals would be permitted to view records of their personal information obtained from the video surveillance system although this is not articulated in Policy B.M.07.

I am therefore satisfied that an individual's ability to access their personal information obtained from the video surveillance system is in accordance with section 36(1) of the *Act*. That said, I suggest that the Board's policy be revised to include wording informing individuals of a right to request their own personal information.

Has the Board 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.

General Security Measures

This provision requires institutions to take reasonable measures to prevent unauthorized access to records in their custody. The *Guidelines* outline the security measures that an institution should take to secure the video surveillance records in their custody and control. The *Guidelines* recommend the following measures:

- Storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area;
- Access to the storage devices should be limited to authorized personnel;
- Audit logs should be kept of all instances of access to and use of recorded information;
- Policies should identify who may view the information; and
- Review should be limited to circumstance where a serious incident has been reported/observed or to investigate a potential crime.

I have reviewed the information provided by the Board 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*.

The Board has also implemented electronic audit logs, detailing accesses to the video surveillance system. The audit log details include date, time, user identification and data accessed.

During the site visit, I observed and confirmed that the digital video recorders containing the information collected from the video surveillance system were located in secure areas with controlled access.

The Board stated and demonstrated its authentication and security measures to control access to the video surveillance system. My site visit confirmed that it had implemented security measures with regards to access controls, including authentication and authorization (password) and that access was limited to senior administrators at the School, as well as facilities and IT staff.

I am therefore satisfied that the Board's security measures with respect to access to the video surveillance system are compliant with section 3(1) of Ontario Regulation 823, made pursuant to the *Act*.

Has the Board implemented retention policies in accordance with section 5 of Ontario Regulation 823, made pursuant to the *Act*?

Section 5 of Ontario Regulation 823, made pursuant to the *Act*, 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 one 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.

With respect to the Board's retention period, the previous version of Policy B.M.07 required that information be retained for 28-42 days but did not address retention periods for video images that have been used. The revised Policy B.M.07 has changed the retention periods as follows:

The retention period for recorded information, which has not been requested or viewed, shall be a minimum of thirty (30) calendar days.

The retention period for recorded information which has been requested for review, shall be a minimum of one (1) year. The records shall be retained in a controlled access location.

Used Records

In cases where images have been accessed and viewed, they would be subject to the one year retention requirement set out above.

The Board confirmed that it does not have a by-law or resolution that sets out an alternative retention period. Instead, as described above, Policy B.M.07 has been revised to address the retention period for used records to ensure compliance with section 5 of Regulation 823, made pursuant to the *Act*.

I have considered the information provided by the Board and I am satisfied, that in the circumstances of this case, the Board has demonstrated that the retention period for used personal information collected by the video surveillance system is in accordance with the *Act*.

Unused Records

In cases where images have not been used, the *Guidelines* state:

Recorded information that has not been used in this fashion [protecting student safety or to deter, detect, or assist in the investigation of criminal activity] should be routinely erased according to a standard schedule. Unused tapes that are not viewed should be erased on a schedule not exceeding one month. The relevant retention periods should be clearly documented in both the board policy and in the board's procedures.

The Board stated that the retention period for images collected through the video surveillance cameras is at least 30 days, and explained that destruction of the information is an automated process.

The Board explained that the video images were retained for a minimum of 30 days due to the operational circumstances that affect when issues may be identified by the School. It was noted that due to the fact that the School is not operational year round, and is often closed for extended periods over the holidays and summer, there may be a delay between when an incident occurs and it being discovered.

I have considered the information provided by the Board and I am satisfied, that in the circumstances of this case, the Board has demonstrated that the retention period for unused personal information collected by the video surveillance system is in accordance with the *Guidelines*.

Policy B.M.07

Although I have found that, with the exception of the collection of personal information from neighbouring properties, the Board's collection, use and disclosure of personal information through use of video surveillance at this School is in accordance with the *Act*, I will comment on Policy B.M.07 and my concerns regarding the framework under which cameras are employed by the Board in its schools generally.

Regarding the principles governing the Board's use of video surveillance, Policy B.M.07 states, in part:

[The purpose is] to ensure that TCDSB assists in maintaining a safe a [sic] secure learning environment for students, staff and community members, by providing appropriate storage and access to video surveillance records.

...

It is correspondingly Board policy to employ video surveillance systems at board schools and facilities only as deemed necessary by the Director of Education, based on available information regarding need and a prudent course of action. Every secondary school shall have a video surveillance system where feasible.

I note that the Board states that it will use video surveillance systems when deemed necessary, yet it also states that every secondary school shall have a video surveillance system where feasible. These statements appear contradictory. In fact, the Board has indicated to me that it is "standard practice" to install cameras in its secondary schools.

I stress that my conclusion that the use of video surveillance at *this* School is necessary is based on recent safety and security events at that facility. I am concerned, however, based on Policy B.M.07, that the Board may have decided to install video cameras at all secondary schools as a default measure rather than based on an assessment of its necessity.

As well, aside from the statement that its goal is to assist in maintaining a safe environment, there is little information in Policy B.M.07 to indicate how the Board will assess whether video surveillance is necessary. Although it alludes to a determination by the Director, Policy B.M.07 does not specify that an assessment of the necessity and utility should be conducted prior to implementing video surveillance at a school. While Policy B.M.07 references the *Act* and the *Guidelines*, it does not identify the factors to consider when determining to implement such a system. Such factors include a history of incidents occurring at a specific school, the physical circumstances of the school and whether video surveillance would be effective in dealing with or preventing future incidents of the type that have already occurred. Absent these factors, or other details regarding what to consider and how to consider it when assessing whether to implement video surveillance, it is not apparent how the Board would determine the "necessity" of using cameras at any given school.

It is therefore my recommendation that the Board's Policy be revised to provide more detailed requirements regarding the decision to initiate use of video surveillance, having regard to the best practices offered in this office's *Guidelines*.

As I have indicated, the Board has already installed video surveillance in all its secondary schools, including the one considered in this Report. Much of the discussion in the *Guidelines*, and the revisions I am recommending, are directed to a decision to initiate the use of video surveillance. However, this does not mean that the principles and best practices described in the *Guidelines* have no relevance here, even where video surveillance has already been established. I will also recommend that the Policy incorporate a process for evaluating the necessity and utility of video surveillance system on an ongoing basis. The *Guidelines* recommend that video surveillance systems be de-commissioned when no longer required or are unable to render the information at the reasonable standard. As noted in MC13-46, the use of video surveillance is not static. Although Policy B.M.07 provides schedules both for maintenance and review of the policy, it does not acknowledge the necessity of periodic evaluations to assess whether video surveillance is necessary. The routine evaluation of the necessity of video surveillance is instrumental to any such activity and it is my recommendation that the Board provide for this in its Policy.

Did the Board Properly Consult With Stakeholders?

As part of his complaint to the IPC, the complainant expressed concern that residents who are neighbours to the School were not consulted prior to the Board's decision to implement the video surveillance system, nor did the Board explain the use and extent of video surveillance. The complainant asserted that the Board did not demonstrate a history of incidents at the School nor were neighbouring residents provided with any information regarding any less intrusive measure that may have been considered prior to the use of video surveillance.

In considering the complaint, I note that there is no requirement under the *Act* to consult specific individuals regarding the collection of personal information if the collection is necessary to the proper administration of a lawfully authorized activity. However, both the *Guidelines* and Policy B.M.07 make it clear that proposals to implement video surveillance systems should involve consultation with the school community, which includes parents, students and staff. Policy B.M.07 states:

In designing and planning the potential use of a video surveillance in an elementary school, or in revising the plan in a secondary school, the Board will ensure that a consultation process will occur with relevant stakeholders at the schools level.

The Board acknowledged that there was no consultation with parents or students regarding the decision to implement video surveillance at the School. The Board explained that because video surveillance had been employed in its secondary schools since at least 1997, it was difficult to provide evidence of demands from stakeholders, such as students, parents and staff.

The matter of consultation raised two questions. First, who are the stakeholders? Second, were they adequately consulted? Addressing the first question, the *Guidelines* recommend open consultation with students, parents, staff and the broader school community. The phrase "broader school community" is not defined in the *Guidelines*, but it is reasonable to conclude that it is

interchangeable with the term “stakeholders” as used by the Board. In the interest of transparency and a generous reading of the term “stakeholders”, it is foreseeable that circumstances would reasonably include additional parties. 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?”

The complainant articulates some of the reasons and criteria for determining who should be consulted. As described above, in certain circumstances it would be prudent and considerate to inform residents in neighbouring properties of security concerns. Communication with neighbours would identify potential issues, such as video surveillance of their property or capturing their comings and goings on the street. It could also both identify potential safety concerns that should be shared with those who may be at risk as well as allay concerns if the video surveillance is implemented in response to issues that do not affect residents. The form of the consultation may vary based on the circumstances.

Regarding the adequacy of the consultation, the Board acknowledges that no such discussions occurred prior to the installation of video surveillance at the School.

It is important to reiterate my comments in Privacy Complaint Report MC13-46: consultation is more than merely announcing the decision to implement video surveillance. An assessment of the necessity of video surveillance would provide an opportunity for stakeholders to provide comments as well as for the Board to communicate its security concerns.

As part of the Board’s assessment regarding the ongoing necessity of the video surveillance system, I expect any further consultation to be consistent with the *Guidelines*, Policy B.M.07 and this Report.

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 from within the School property is in accordance with section 28(2) of the *Act*.
3. The collection of the personal information from outside of the School property is not in accordance with section 28(2) of the *Act*.
4. The Board has not provided Notice of Collection in accordance with section 29(2) of the *Act*, and the IPC’s *Guidelines*.
5. The Board’s use of the personal information is in accordance with section 31 of the *Act*.
6. The Board’s contemplated disclosure of the personal information is in accordance with section 32 of the *Act*.

7. The Board permits access to personal information in accordance with section 36 of the *Act*.
8. The Board has implemented reasonable measures to protect the security of personal information as required under section 3(1) of Ontario Regulation 823, made pursuant to the *Act*.
9. The Board's retention period for unused personal information accords with the *Guidelines*.
10. The Board's retention period for used personal information accords with section 5 of Ontario Regulation 823, made pursuant to the *Act*.

RECOMMENDATIONS

1. I recommend that the Board cease collection of personal information obtained by the video surveillance system from outside of the School property.
2. I recommend that the Board revise its Notice of Collection in accordance with section 29(2) of the *Act*, and as outlined in this Report.
3. I recommend that the Board revise its policies, procedures and guidelines to reflect the recommendations in the *Guidelines* and this Report, including providing clear and detailed information regarding the implementation and operation of video surveillance within its schools and provisions for periodic review of the continuing necessity for the video surveillance, having regard to the best practices described in the *Guidelines*.

The Board has reviewed this Report and agrees to implement the recommendations described above. Within two weeks of publication of this Report, the Board undertakes to implement Recommendation 1. Within 30 days of publication of this Report, the Board undertakes to give the Information and Privacy Commissioner a written plan setting out its steps to comply with Recommendations 2 and 3.

Original Signed by: _____

Jeffrey Cutler
Investigator

July 17, 2015 _____