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 MC13-46

Halton Catholic District School Board

March 11, 2015

Summary: The complainant, whose child attended the St. Thomas Aquinas Catholic School in Oakville (the School), expressed concern with the use of video surveillance at the School, which is operated by the Halton Catholic District School Board (the Board). The Office of the Information and Privacy Commissioner/Ontario (the IPC) finds that the Board's collection of the personal information is not in accordance with section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act)*. The IPC recommends that the Board conduct an assessment of the video surveillance system at the School in a manner consistent with the *Act*, the Board's internal policy and this Report.

With consideration that the Board may determine that video surveillance at the School is in accordance with section 28(2) of the *Act*, this Report also considers whether the Board's use, disclosure and retention of personal information is in compliance with the *Act.*

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 and MC10-2.

Cases Considered: *Cash Converters Canada Inc. v. Oshawa (City)*, (2007) 86 O.R. (3d) 401; *Eastmond v. Canadian Pacific Railway,* [2004] F.C.J. 1043; *Alberta Order P2006-008*, [2007] A.I.P.C.D. No. 16; *Shoal Point Strata Council (Re)*, 2009 CanLII 67292 (BC IPC).

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 Halton Catholic District School Board (the Board).

The complainant, whose child attended the school, became aware of the use of video surveillance cameras at St. Thomas Aquinas Catholic School in Oakville (the School). The complainant expressed concern with the use of video surveillance at the school, and the alleged lack of consultation with parents and students regarding its implementation. The complainant explained that she expressed her concerns to the Director of the Board, four school trustees and the school itself. The Board's Director of Education responded to complainant in a letter dated May 7, 2013 in which he explained the decision to implement video surveillance at all of the Board's secondary schools.

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 over one thousand students. The Board also provided our office with a copy of the relevant policy titled "I-30: Operating Policy: Video Surveillance" (Policy I-30), as well as background documentation.

In its response to the complainant, the Board explained that a committee consisting of secondary school principals and Board staff was established in February 2010 to examine the need for video surveillance systems at all of its secondary schools. The Board explained that the objective was "to improve the safety and security of student, staff, visitors and Board property." In June 2011, the Board approved the "Proposed Secondary Schools Video Surveillance Camera System Project" for implementation in all of its secondary schools. Subsequently, new video surveillance systems were installed in these schools during 2011 and 2012.

The Board explained that in March of 2012, 53 internal video cameras and 9 external video 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.

The Board indicated that it has signs 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 IPC's *Guidelines for Using Video Surveillance Cameras in Schools*[1] (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 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 in 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*, MC07-68[2] and Privacy Complaint Report MC10-2[3]]. The Board agrees that the

[1] www.ipc.on.ca/images/Resources/vidsch-e.pdf
[2] http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf
[3] www.ipc.on.ca/images/Findings/MC10-2.pdf

information collected from the video surveillance cameras qualifies as "personal information" under the *Act*.

Based on the above, I concur 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*.

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 circumstance, 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. The Board states that its operation of the School is lawfully authorized by virtue of section 170(1) of the *Education Act* and I agree. The 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 next question to consider is whether the collection of images through the video surveillance system is necessary to the operation of the School. Both the *Guidelines* and the Board's Policy I-30 provide direction regarding the necessity of video surveillance programs in schools.

In *Cash Converters Canada Inc. v. Oshawa (City)*[4] the Ontario Court of Appeal adopted the following approach with respect to the application of the necessity condition and stated:

> In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the *Act*. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.[5]

This approach was adopted in *Special Investigation Report*, MC07-68 and Privacy Complaint Report MC10-2 and incorporated into the *Guidelines*. In *Special Investigation Report*, MC07-68, Commissioner Cavoukian concluded:

> 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.

The IPC *Guidelines* acknowledge that in certain circumstances, the use of video surveillance in schools may be permissible under the *Act*. The *Guidelines* recommend that before deciding to use a video surveillance system, that school boards consider the following:

- Video surveillance should only be considered where less intrusive means of deterrence, such as increased monitoring by teachers, have shown to be ineffective or unworkable;

- In its consultation with the school community, the board should outline the less intrusive means that have been considered and the reason why they are not effective;

- Before implementing a video surveillance program, a school should be able to demonstrate:

    - a history of incidents occurring in the specific school;

[4] *Cash Converters Canada Inc. v. Oshawa (City)*, (2007) 86 O.R. (3d) 401.
[5] Ibid, at para. 40.

  - the physical circumstances of the school – does it permit ready access to unauthorized individuals; is there a history of intrusion by unauthorized individuals; are there specific safety issues involving that school;

  - whether a video surveillance program would be effective in dealing with or preventing future incidents of the type that have already occurred;

- Video surveillance programs should only be adopted where circumstances have shown that it is necessary for the purposes of providing the safety of students and staff, or for the deterrence of destructive acts, such as vandalism;

- The board should provide justification for the use and extent of a video surveillance program on the basis of addressing specific and significant concerns about safety and/or the theft or destruction of property;

- The board should conduct an assessment into the effects that the surveillance system will have on personal privacy and the ways in which such adverse effects may be mitigated;

- The board should consult openly with parents, staff, students and the broader school community as to the necessity of the proposed video surveillance program and its acceptability to the school community. Consultation should provide stakeholders with an opportunity to comment on the actual location of cameras on school property, should the project proceed; and,

- The board should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is necessary to achieve appropriate goals through lawful activities.

As noted in the *Guidelines*, "Where the collection of personal information would merely be helpful to the board, it is not 'necessary' within the meaning of the *Act*".[6]

Policy I-30 is consistent with the *Guidelines*. Regarding the principles governing the Board's use of video surveillance, the Policy states, in part:

> The Board holds that under the *Education Act*, schools are considered to be supervised environments where reasonable monitoring of the activity of all persons is both desirable and expected.

[6] See *Cash Converters Canada Inc. v. Oshawa (City)*, (2007) 86 O.R. (3d) 401, at paragraph 40.

…

> The Board does not endorse the use of video surveillance systems as an acceptable substitute for the in-person supervision of students by school staff as assigned by the school principal. Video surveillance systems may be an appropriate and useful tool with which to augment or support the assigned in-person supervision provided by staff.
>
> The Board accepts that the lawful, controlled, limited, purposeful and supervised use of video surveillance may be an important resource for maintaining order and discipline on Board sites, and may include but is not limited to the control of theft and vandalism, and the investigation of other criminal activity perpetrated by any person(s).
>
> …
>
> Video surveillance programs shall only be adopted where it is necessary for the purposes of enhancing the safety of students and staff, or for the deterrence of unauthorized access and destructive acts, such as vandalism and theft.
>
> Video surveillance systems will be de-commissioned when no longer required or are unable to render information at the reasonable standard.

The Policy also outlines the following requirements with respect to collection, stating, in part:

> Proposals for the installation and use of video surveillance systems on any Board site for the approval of the Administrative Council of the Board must demonstrate:
>
> - that the collection of such personal information is authorized under the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*;
> - that less intrusive means of deterrence, such as increased monitoring by staff, have been shown to be ineffective or unworkable;
>
> …
>
> - that an assessment has taken place of the effects the surveillance system would have on personal privacy;

- that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required lawful goals;

…

- that video surveillance will not be possible in locations where staff and students have a reasonable expectation of privacy such as washrooms, shower rooms, change rooms.

Special Investigation Report, MC07-68, considered the use of video surveillance in the context of the Toronto Transit Commission (TTC) and mass transit. In concluding that the video surveillance was necessary, Commissioner Cavoukian considered a range of information, including studies and information from other jurisdictions that considered the role and utility of video cameras in providing security on mass transit systems. Commissioner Cavoukian noted considerations such as assaults on TTC staff, crime, terrorism concerns and the general need to manage large volumes of people and equipment in a safe and secure manner.

When assessing 'necessary' in the context of video surveillance, a review of decisions in other jurisdictions is of assistance. In *Shoal Point Strata Council (Re)*[7], the Information and Privacy Commissioner of British Columbia considered the decision of a private condominium corporation to implement video surveillance cameras at a residential property. *Shoal Point* includes an analysis of the Federal Court's decision in *Eastmond v. Canadian Pacific Railway*[8] and an order of the Alberta Privacy Commissioner, decision P2006-008[9].

In concluding that the corporation should not have been collecting video surveillance to the degree which they had, the B.C. Privacy Commissioner noted the following:

- The sensitivity of personal information captured by video surveillance is variable, and that viewed cumulatively or over time, video images can convey sensitive details of the habits and lifestyle of individuals.

- No evidence to demonstrate legitimate security concerns prior to implementation was established. The video surveillance systems were installed during construction and were incorporated into the building design and prior to evidence of security threats. As well, the

[7] *Shoal Point Strata Council (Re)*, 2009 CanLII 67292 (BC IPC).
[8] *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. 1043.
[9] *Alberta Order P2006-008*, [2007] A.I.P.C.D. No. 16.

corporation failed to demonstrate that there would be a reasonable expectation of security breaches upon construction. The decision notes that the use of video surveillance was based on an assumption, unsupported, of any security threat.

- The security concerns were comparatively minor as compared to *Eastmond* and P2006-008.

- There was a "paucity of substantial evidence to justify" the implementation of video surveillance. Other than the installation of cameras by specific entrances, the implementation of video surveillance was determined to have been pre-emptive and not in response to demonstrated problems. Furthermore, the reported incidents that have occurred are not exceptional and are spread over several years.

- Video records should only be viewed if there is a legitimate safety or security incident or threat.

I note that the decision in *Shoal Point* appears to accept the use of video surveillance at entrance points more readily than internal cameras. In that circumstance, the distinction was between demonstrative external threats versus internal safety and bylaw enforcement issues, for which there was little evidence presented to the B.C. Privacy Commissioner to support the use of video surveillance when less intrusive measures could have been employed.

In *Eastmond v. Canadian Pacific Railway,* the Federal Court considered the use of video surveillance in the workplace context and the application of the *Personal Information Protection and Electronic Documents Act*. The Court upheld the company's use of video surveillance at a railway maintenance facility and overturned the Office of the Privacy Commissioner of Canada decision ordering its removal. The Court concluded that there was evidence to demonstrate that there was a significant problem that could not be addressed by other means, and noted the following considerations:

- The video surveillance was installed at a large site;

- 148 security and safety incidents over a 5 year period;

- The personal information obtained from the cameras was limited;

- Cameras were located only at the two entry points;

- Access to the records was restricted and limited;

- Records were not viewed unless there was an incident requiring investigation; and

- Images retained for 96 hours.

In Alberta Order P2006-008, Commissioner Frank Work upheld the use of video surveillance cameras at a private fitness centre. Commissioner Work considered the reasonableness of the purposes to which the information was collected in the context of section 11(1) and (2) of Alberta's *Personal Information Protection Act*. Specifically, Commissioner Work considered:

- The nature of the information collected;

- The purposes and circumstances surrounding collection and use of the information; and

- How the organization handles the information (minimal level of intrusiveness of the measures. The Commissioner noted that video cameras that monitor and record are the most intrusive, and the least intrusive are cameras that record without monitoring).

In the above case there had been approximately 900 incidents of theft and property damages over a 3 year period at the fitness centre prior to installation of the video cameras. The fitness centre had tried other measures without success and demonstrated that security incidents declined 400% following the implementation of cameras.

Commissioner Work noted the following:

- The level of theft and property damage created a legitimate issue and the organization attempted to find alternative solutions before resorting to video surveillance. The organization provided satisfactory explanations as to why these measures had not worked;

- The video surveillance was restricted to areas that were the subject of theft and damage;

- The cameras were not actively monitored;

- The information obtained from the video cameras was only reviewed when there was criminal activity that had been reported to the police and a police file generated;

- The limitations on the capabilities and usage of the surveillance system limited the privacy intrusion to an appropriate level; and

- Access to the images was limited to a few personnel and then only in the event of a reported incident.

Turning to the circumstances in this complaint, the Board's decision to install video surveillance at the School was part of a larger initiative to implement such systems in all of its secondary schools. This decision was made in June 2011, when the Board approved the Proposed Secondary Schools Video Surveillance Camera System Project. The objective was "to improve the safety and security of student, staff, visitors and Board property."

As indicated in the information provided by the Board, implementation of the video surveillance system arose at the Catholic School Council. A review of the November 7, 2011 School Council Agenda and Minutes makes reference to the intention to install "security cameras". The Agenda also notes the following:

- Question asked about thefts in schools – doesn't seem to be any more or less than previous years.

- Report of some theft in the locker room at the beginning of the year.

In response to whether the cameras were located in "necessary locations" (minimizing collection of [Personal Information] to that which is reasonably necessary to fulfillment of a lawfully authorized activity), the Board responded:

> Yes, the cameras were located throughout the building in consultation with the Facilities Services Department, the Principal and the Consultant. [They] were placed in common areas, such as hallways, entrances and outside to assist us in ensuring the ongoing safety of our staff, students, visitors and the protection of our property.

Policy I-30 outlines the purposes for which video surveillance in schools shall be conducted. To summarize, it is to enhance the safety of students and staff and the protection of school property. The information provided by the Board, and obtained during my site visit, confirms that the video surveillance system does not capture personal information from classrooms, washrooms, showers and change rooms. With the exception of classrooms, these are areas that both Policy I-30 and the *Guidelines* identify as having expectations of privacy.

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 is 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 the 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.

In response to this investigation, the Board provided a list of incidents at the School that involved the use of the video surveillance system since its implementation in March 2012. The list is comprised of 17 incidents over a period of two years. In five of these circumstances the Board determined that no useful information could be recovered from the video surveillance system. In the remaining 12 incidents the Board determined that useful information was obtained from the video cameras. The 12 incidents that provided useful information may be generally described as involving physical/verbal altercations between students, one reported incident of drug use on school property, theft and student pranks.

Whether these circumstances merit the necessity of video surveillance at all, or particularly at the level of intensity employed by the Board at the School, I turn to the framework articulated in *Shoal Point*, which states:

> Decisions about whether to implement video surveillance should not be swayed unduly by the general appeal of technological solutions. They should be based on an assessment, in the circumstances of each case, of the real need for surveillance of this kind, its reasonably expected benefits and the impact of its use on privacy. Video surveillance should be used only in response to a real and significant security or safety problem. In saying this, I note as an aside that one of the inherent risks of video surveillance is "function creep", which is the extension of the uses of a technology beyond the use for which it was implemented in the first place. There are cases, for example, in which surveillance cameras originally installed to deter burglary were subsequently used to enforce minor infractions.

When applying the observations in *Shoal Point*, as well as those of the Federal Court in *Eastmond v. Canadian Pacific Railway* and the Alberta Privacy Commissioner in Order P2006-008, to the circumstances of this complaint, I note that with the exception of the one episode of drug use on school property, the reported incidents do not appear exceptional, either in terms of their severity or frequency.

The final matter to address regarding the Board's collection of personal information is the process of ongoing evaluation. Policy I-30 states that "[video] surveillance systems will be de-commissioned when no longer required or are unable to render the information at the reasonable standard." This makes clear that the use of video surveillance is not static, and that the onus is on the Board to determine the necessity and utility of video cameras. I note that the Board explained that it forwards the logs for the video surveillance system to the Family of Schools Superintendent at the end of each school year for "review", but it is not clear how this review is conducted to determine the ongoing necessity of the video surveillance system. Absent a privacy impact assessment or similar type of analysis, it is not apparent how such a review actually evaluates the necessity and effectiveness of the video surveillance system.

Having reviewed all the information before me, I am not 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*.

While Policy I-30 is reflective of the *Guidelines*, the information before me indicates that the Board did not adhere to its own policy in practice. I stress that the IPC expects more than mere acknowledgement of an institution's obligations under the *Act*; it expects institutions to act upon their obligations. Specifically, the Board did not demonstrate that video surveillance at the School was necessary and implemented in a manner consistent with either the *Guidelines* or Policy I-30. Nor has it demonstrated that it has the measures in place to adequately evaluate the necessity and utility of the video surveillance system on an ongoing basis.

It is important to stress that I am not concluding that the use of video surveillance at the School is not necessary per se. Rather, I conclude that the Board *has not demonstrated* that it is necessary, or even necessary to the degree with which it has been implemented. Therefore, I will recommend that the Board conduct an assessment of the video surveillance system at the School in a manner consistent with the *Act*, Policy I-30 and this Report. If it determines, following an assessment of the video surveillance system, that it is necessary, I will recommend that the Board implement the video surveillance system at the School in a manner consistent with the *Act*, Policy I-30 and this Report.

Findings regarding the Board's use, disclosure and retention of personal information are contingent on the valid collection of personal information and, given my determination

above, may not be strictly necessary at this time. However, these additional issues have been put squarely before me and my findings on them will be applicable if, following an assessment, the Board determines the system is necessary and implemented in a manner consistent with Policy I-30 and this Report. As well, the results of this investigation and an analysis of the Board's efforts to comply with the *Act* will be instructive to the Board, stakeholders and other institutions. Therefore, with consideration that the Board may determine that video surveillance is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*, I will now also consider whether the Board's use, disclosure and retention of personal information is in compliance with the *Act*.

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 advised that it had signs in place at the entrances to the School. The signs initially stated "SECURITY NOTICE: THIS PROPERTY IS PROTECTED BY ELECTRONIC SURVEILLANCE". In response to recommendations from this office during my investigation, the Board has revised the notice to state:

> 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 Halton Catholic District School Board property. 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 905-632-6300.

The Board provided the IPC with a copy of the revised notice.

Having reviewed the revised notice provided by the Board, I am satisfied that it meets the notice requirements set out in section 29(2) of the *Act*.

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 I-30 outlines the uses of the personal information obtained through its video surveillance. I have identified the following excerpts from Policy I-30 that describe both permissible and impermissible uses:

- The Board accepts that the lawful, controlled, limited, purposeful and supervised use of video surveillance may be an important resource for maintaining order and discipline on Board sites, and may include but is not limited to the control of theft and vandalism, and the investigation of other criminal activity perpetrated by any person(s).

- Video surveillance programs shall only be adopted where it is necessary for the purposes of enhancing the safety of students and staff, or for the deterrence of unauthorized access and destructive acts, such as vandalism and theft.

- The Board reserves the right to limit or exclude uses of video surveillance that are not compatible with the Church's views on the dignity of the human person.

- The Board does not support the use of information obtained through video surveillance for the purpose of routine staff performance appraisal or monitoring. This excludes the covert use of video surveillance for investigating possible criminal activity.

- The Board reserves the right to consider and employ lawful "covert surveillance" on a case by case basis in consultation with the appropriate police service.

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.

The Board states that the uses of the personal information obtained from the video surveillance system are in accordance with section 31 of the *Act* and they are not used for purposes outside of those listed in Policy I-30. Board staff at the School who are authorized to access the video surveillance system reiterated this position during my site visit. Furthermore, a review of the logs pertaining to the video surveillance system indicate uses that are consistent with the Board's stated position.

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. All of these purposes relate to the proper administration of a school.

The uses of personal information listed above relate to safety, security of the property, and investigations of criminal activity. In my view, these uses are all elements of the proper administration of a school, which is the original purpose of the collection.

Therefore, pending a determination that the Board's collection of personal information via the video surveillance system is in accordance with section 28(2) of the *Act*, 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*.

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

Policy I-30 identifies 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 now address each of the two potential disclosures of personal information identified in the Board's Policy I-30.

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. 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.

I note that the type of uses of the video surveillance system as described in Policy I-30 (e.g., to control and investigate thefts, vandalism and other criminal activities) 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*.

The second type of disclosure contemplated by Policy I-30 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 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*?

Policy I-30 acknowledges the rights of individuals to request access to their personal information as contained in records arising from the video surveillance system.

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 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. Furthermore, Policy I-30 explicitly states that:

> Any student, staff member or member of the public that has been recorded by a video surveillance camera has a general right of access to his or her personal information under section 36 of the Municipal Freedom of Information and Protection of Privacy Act. Access may be granted to one's own personal information in whole or in part, unless an exemption applies under section 38 of the Municipal Freedom of Information and Protection of Privacy Act.

I note that the access guidelines described in Policy I-30 acknowledge the right of access to personal information.

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*.

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*.

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

A storage log is maintained by the Board. The log describes incidents of access and use, including date, time and purpose as per Policy I-30. The log books are forwarded to the Family of Schools Superintendent at the end of each school year for review.

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.

With respect to access to images taken from the video surveillance system, Policy I-30 states:

- Access is limited to authorized personnel with specific duties pertaining to the supervision, operation and maintenance of the video surveillance system and for the proper, secure storage and destruction of video recordings.

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.

With respect to system reviews and audits, the Board stated that the audit logs are generated by individuals accessing the video surveillance system. The logs are not generated by computer; rather, they are hand written and record the date, describe the incident under review, the information captured by the video surveillance system and the outcome.

While user created logs are helpful, this is not an optimal security measure because it will not capture surreptitious access. I acknowledge that neither the *Guidelines*, nor Policy I-30 specify the format and method of logging, and that the Board's practice is in keeping with these documents.

Staff Training and Confidentiality Agreement

While the *Guidelines* reference the requirement for education and training for individuals with access to video surveillance systems in schools, Policy I-30 does not address this requirement. The Board explained in its submissions that its facilities department provides basic operating instructions to the school administrator. During my site visit, staff confirmed that they were aware of the confidential nature of the information obtained from the video surveillance system and of the measures to maintain the security of the video surveillance system.

Policy I-30 directs that staff and service providers with duties related to the operation of the video surveillance system are to sign confidentiality agreements. Specifically its states that "Board employees and the employees of service providers performing any duties related to the operation of a Board approved video surveillance program are required to sign an undertaking of confidentiality." Underlying this requirement is the

statement under the "Principles" section of Policy I-30 that "[t]he Board supports the adoption of an oath of confidentiality by those whose function it is to deal with the day-to-day operation of video surveillance systems."

The Board acknowledges that staff with access to the video surveillance system at the School are not required to sign an undertaking of confidentiality as recommended in the *Guidelines* and Policy I-30.

Based on the above, I am satisfied that the Board has met its obligations under section 3(1) of Regulation 823, made pursuant to the *Act*. That said, as a means to optimize security and accountability, I will recommend the following:

- The Board explore, and if feasible, implement measures that automatically log user activity with respect to the access and use of the video surveillance system instead of relying upon user self-reporting.

- The Board undertake to have all relevant staff and service providers sign a confidentiality agreement with regards to access to the video surveillance system as per the *Guidelines* and Policy I-30.

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 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, Policy I-30 states:

> A timetable for the retention, storage and destruction of video surveillance media and storage log books will be established under the advice of Board

> legal counsel and be strictly adhered to at each site employing video surveillance.

In cases where images have been accessed and viewed, they would be subject to the one 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 [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.

Unused Records

The Board stated that the retention period for images collected through the video surveillance cameras is approximately 14 to 20 days, after which new information is recorded over the older data. The retention period varies between 14 to 20 days depending on the amount of activity being recorded and the storage space available on the hard drives.

The Board explained that the video images were retained for a minimum of 14 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*.

Used Records

Regarding images that are used (viewed), the Board explained that:

> Typically the images are not copied or saved unless requested by Police or the Administration. They are then retained as part of the file for the particular situation (i.e. suspension or expulsion of a student or a police investigation) they will be retained for an indefinite period of time depending on the situation.

After carefully reviewing Policy I-30 and the Board submissions, it is not apparent that the retention period is consistent with the one year requirement prescribed by section 5 of Regulation 823, made pursuant to the *Act*. The Board stated that it does not have a by-law or resolution that sets out an alternative retention period. Nor is there a timetable for the retention, storage and destruction of video surveillance media as referenced in Policy I-30.

In order to ensure full compliance with the retention period outlined in section 5 of Regulation 823, I will recommend the following:

- The Board's policies/procedures/guidelines should be revised to reflect the specific timelines for retaining information from the video surveillance system that it has used.

I note that the Board has undertaken to develop a timetable as per Policy I-30. The Board states that staff are made aware of the retention requirements set out in Policy I-30 through the local supervisor and working with the system.

Did the Board Properly Consult With Stakeholders?

In presenting her complaint to the IPC, the complainant expressed concern that parents and students were not consulted prior to the Board decision to implement the video surveillance system.

In considering this part of 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 I-30 make it clear that proposals to implement video surveillance systems should involve consultation with the school community, which includes parents, students and staff. Policy I-30 provides additional detail, stating:

> Proposals for the installation and use of video surveillance systems on any Board site for the approval of the Administrative Council of the Board must demonstrate:
>
> …
>
> - that consultation with the school community has taken place through the Catholic School Council, with the broader community of parents, staff, and students regarding the acceptability of video surveillance on the site. Consultation should provide stakeholders with an

> opportunity to comment on the actual location of cameras should the project proceed.

The Board contested the complainant's assertion that there was a lack of consultation. The Board explained that the School Council Agenda dated November 7, 2011, the staff meeting dated December 6, 2011 and the Parent Council meeting dated April 10, 2012, identify the implementation of the video surveillance system as items for discussion. That said, it is not apparent that the Board's consultations meet the criteria referenced in both the *Guidelines* and Policy I-30. For example, the information provided by the Board indicates that the process consisted of providing information regarding the status of implementation of the video surveillance system, as opposed to consultations with stakeholders regarding this initiative. There is no indication that stakeholders were provided an opportunity to comment on the location of the cameras or to even assess their necessity. Absent an assessment of the necessity of video surveillance, it is not clear what information has been presented to stakeholders to inform their consultation, aside from a reference to a recent theft and a comment that security incidents have been no more or less frequent.

Based on the above, I am satisfied that the Board did inform stakeholders of its intention to implement video surveillance at the School. However, as part of the Board's assessment regarding the necessity of the video surveillance system, I expect any further consultation to be consistent with the *Guidelines* and Policy I-30.

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 not in accordance with section 28(2) of the *Act*.

> With consideration that the Board may determine that video surveillance is necessary to the proper administration of a lawfully authorized activity in accordance with section 28(2) of the *Act*, I will now also consider whether the Board's use, disclosure and retention of personal information is in compliance with the *Act.* An analysis of the Board's efforts to comply with the *Act* will also be instructive to the Board, stakeholders and other institutions. Therefore, pending a determination that the Board's collection of personal information via the video surveillance system is in accordance with section 28(2) of the *Act*, I find:

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

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

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

6. The Board permits access to personal information in accordance with section 36 of the *Act*.

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

8. The Board's retention period for unused personal information accords with the *Guidelines*.

9. The Board's retention period for used personal information does not accord with section 5 of Ontario Regulation 823.

10. The Board did inform stakeholders of its intention to implement video surveillance at the School. However, as part of the Board's assessment regarding the necessity of the video surveillance system, I expect any further consultation to be consistent with the *Guidelines* and Policy I-30.

RECOMMENDATIONS

1. I recommend that the Board conduct an assessment of the video surveillance system at the School in a manner consistent with the *Act*, Policy I-30 and this Report.

2. Following an assessment of the video surveillance system and assuming a determination that it is necessary, I recommend that the Board implement the video surveillance system at the School in a manner consistent with the *Act*, Policy I-30 and this Report.

3. I recommend that the Board explore, and if feasible, implement measures that automatically record user activity with respect to the access and use of the video surveillance system instead of relying upon user self-reporting.

4. I recommend that the Board undertake to have all relevant staff and service providers sign a confidentiality agreement with regards to access to the video surveillance system as per the *Guidelines* and Policy I-30.

5. I recommend that the Board revise its policies, procedures and guidelines to reflect the specific timelines for retaining information from the video surveillance system that it has used.

The Board has reviewed this Report and agrees to implement the recommendations described above. Within 60 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 all of the recommendations.

Original Signed By: March 11, 2015
Jeffrey Cutler
Investigator