Office of the Information and Privacy Commissioner for Nova Scotia

INVESTIGATION REPORT IR17-01

Video Surveillance at the Cape Breton-Victoria Regional School Board

Catherine Tully
Information and Privacy Commissioner for Nova Scotia
October 12, 2017

TABLE OF CONTENTS

	Page
Commissioner's Message	3
Executive Summary	5
1.0 Purpose and Scope	7
1.1 Background	7
1.2 Jurisdiction	7
1.3 Investigative process	8
2.0 Issues	9
3.0 Analysis and Findings	9
3.1 Why is privacy important?	9
3.2 Does the Board have reasonable security in place for the video surveillance system at Rankin School?	10
a. Installation	11
b. Purposes	11
c. Security of video surveillance system	12
d. What is reasonable security?	12
e. Security of video surveillance at Rankin School	13
f. Were reasonable steps taken in response to the breach?	15
3.3 Is the Board authorized to collect personal information through video surveillance?	24
a. Video surveillance in Nova Scotia's schools	24
b. Why is the Board conducting video surveillance at Rankin School?	25
c. When is collection of personal information through video surveillance authorized?	25
4.0 Summary of Findings and Recommendations	36
5.0 Conclusions	38
6.0 Acknowledgements	39
Appendix 1	41
Appendix 2	47
Bibliography	49

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Catherine Tully

INVESTIGATION REPORT

October 12, 2017

Cape Breton-Victoria Regional School Board

Commissioner's Message

There is no question that the safety of our children is of fundamental importance to Nova Scotians. As video surveillance tools have gotten cheaper and easier to use, school boards across Nova Scotia and around the world have installed video surveillance. They generally cite the need to ensure the safety of the children as the reason for the use of video surveillance.

Video surveillance is highly privacy invasive. It allows authorities to watch us, sometimes overtly and sometimes covertly. But as our courts have said, privacy is at the heart of liberty in a modern state. Children, school staff, visitors and parents are all entitled to privacy, even in public spaces. The Department of Education's own material recognizes that oppressive security can impart a message to children that they are not trusted. This can in turn decrease the sense of attachment and engagement that the Department recognizes is essential for student achievement.

This investigation highlights two significant concerns with video surveillance in Nova Scotia's schools. First, it is essential that if video surveillance is used, it must be properly secured. When video surveillance images from the Rankin School were streamed on the internet for all to see this was a violation of Nova Scotia's privacy laws. The camera feeds showed when students entered and exited the school, and when male students entered the washroom, alone or in groups. This information, streaming unsecured to the Internet, created a risk to student safety. It also exposed them to potential embarrassment or humiliation.

Second, it is essential that school boards conduct a thorough privacy impact assessment of their video surveillance systems in order to find the proper balance between ensuring the safety of children while respecting their privacy. In Nova Scotia school boards across the province have implemented video surveillance without conducting any privacy impact assessment of their surveillance – the Cape Breton-Victoria Regional School Board is no exception. The way

forward is for school boards around the province to join together to conduct a thorough privacy impact assessment so that video surveillance is designed to meet the safety requirements while respecting the fundamental right to privacy that all citizens, including children, are entitled to.

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Executive Summary

[1] In May 2017, CBC News reported that a Russian website had posted a link to live video feeds from surveillance cameras at the Rankin School of the Narrows (Rankin School) in Iona, Nova Scotia. As a result, images of Cape Breton school children were accessible to viewers around the world.

[2] The Cape Breton-Victoria Regional School Board (Board) is responsible for ensuring that the Rankin School is compliant with the privacy rules set out in the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*).

[3] On learning of the incident, the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) immediately contacted the Board and initiated a privacy breach investigation. Our investigation revealed that the Board had failed to adequately secure its video surveillance cameras. We identified two basic security weaknesses that contributed to the privacy breach: a failure to use unique, robust, complex passwords and a failure to secure against a common technical security vulnerability that results when one internet-connected device allows unauthorized access to other similar devices or entire databases. This is known as an insecure direct object reference. This second security failure allowed visitors to the Russian website to access not only the one school camera whose link was posted to the website, but all three of the Rankin School cameras.

[4] The Board's initial response to the breach – changing all camera passwords – was sufficient to contain the breach. However, significant further work is required to prevent future breaches from occurring. As a result, I recommend a number of improvements to the Board's technical security arrangements, development of appropriate privacy policies and procedures and further staff training.

[5] The camera initially available via the Russian website link is a camera located in the hallway outside the boys' washroom at Rankin School. The Board explained that this camera was installed in response to a specific incident in 2015. That matter resolved in 2015. Collection of personal information via video surveillance must comply with the rules in *FOIPOP*. The Board offered no explanation or argument to justify the ongoing use of this video camera under *FOIPOP*. As a result, I recommend that this washroom entrance camera be disabled.

[6] During the course of our investigation, we discovered that while every school board in Nova Scotia has implemented some level of video surveillance, no board has conducted a privacy impact assessment to ensure that the surveillance is in compliance with our privacy laws. The Cape Breton-Victoria Regional School Board is no exception. Therefore, I recommend that the school boards work together to develop a privacy impact assessment for video surveillance in schools. Such an effort will ensure that the privacy rights of students, staff, parents and visitors are respected while ensuring the safety of children and staff. To aid in this effort, my office will organize a privacy impact assessment workshop in the coming months. All school boards in Nova Scotia, except the Cape Breton-Victoria Regional School Board, have agreed to participate in this effort.

[7] In summary, I make six recommendations:

1. That the Board develop its own privacy breach policy.
2. That the Board further secure its cameras either behind a firewall or by another equivalent technical strategy.
3. That the Board replace its two exterior cameras which are no longer supported by the manufacturer once it has completed a privacy impact assessment.
4. That the Board update its policies and practices to include privacy training, updated confidentiality agreements, mandatory audits of video surveillance, a Board specific breach policy and a password policy.
5. That the Board immediately disable the video surveillance camera outside of the boys' washroom at Rankin School.
6. That the Board conduct a privacy impact assessment of its video surveillance system and provide the OIPC with a copy.

1.0 Purpose and Scope

1.1 Background

[8] On May 4, 2017, CBC News reported that a Russian website was posting the link to live video feeds from the surveillance cameras at the Rankin School of the Narrows in Iona (Rankin School), Nova Scotia. The CBC News story included still photos taken from the video streams. The stills clearly showed children clustered around a water fountain and washroom entrance. CBC News noted in its story that it had blurred the images of the children, but that they were clearly visible in the videos it had looked at. The CBC News story also reported that "several cameras" captured the school's parking lot, playground and bus loop, and exit doors from the school. The story was accompanied by three screen captures of images of the school's yard, and one of the doors. It was unclear from the story precisely how many cameras were accessible on Insecam.org.[1]

[9] The same day, staff from the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) contacted representatives of the Cape Breton-Victoria Regional School Board (Board).[2] The OIPC indicated we would be initiating an investigation into the Board's privacy practices surrounding video surveillance at Rankin School. We confirmed that the passwords to all cameras had been changed. We further confirmed that the Board had checked the Insecam site to confirm that the original link no longer worked. We provided some guidance on what the Board should consider when investigating the breach, and recommended that the Board shut down all its cameras until it could satisfy itself that the breach had been properly investigated. We later learned that the Board did not shut down the cameras, nor was it prepared to do so because it was under the belief that the password changes were sufficient to adequately secure the cameras.

[10] Our investigation revealed that Rankin School had three internet protocol (IP) video surveillance cameras installed. Rankin School has a fixed camera mounted across the hall from a water fountain and boys' washroom, and another fixed camera above the main entry doors to the school. The third camera is a pan-tilt-zoom camera installed on an exterior corner of the building. It provides views of the bus turning loop, parking lot and playground through its regular arc.

1.2 Jurisdiction

[11] The Board is a public body pursuant to the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*).[3] The Board's collection, security, use and disclosure of personal information must comply with *FOIPOP* ss. 24 through 31. The *Education Act* gives the Board authority for the overall management of the Rankin School.

---

[1] "Russian website broadcast live pictures of Cape Breton schoolchildren," May 4, 2017, CBC Nova Scotia. Available online at: http://www.cbc.ca/news/canada/nova-scotia/rankin-school-students-security-video-camera-russian-website-1.2762291.

[2] The Rankin School of the Narrows falls under the responsibility of the Cape Breton-Victoria Regional School Board.

[3] Section 3(1)(j) of *FOIPOP* sets out the definition of public body which includes a "local public body". Local public body is further defined in s. 3(1)(ea) of *FOIPOP* to include a school board as defined in the *Education Act*.

[12] Under the *Privacy Review Officer Act* (*PRO*), the Commissioner has a statutory mandate to monitor compliance of public bodies with *FOIPOP* to ensure the purposes of the legislation are achieved. The relevant purposes, as stated in s. 2 of *FOIPOP*, are "to ensure that public bodies are fully accountable to the public by preventing the unauthorized collection, use or disclosure of personal information by public bodies, and…to protect the privacy of individuals with respect to personal information about themselves held by public bodies."

[13] Pursuant to *PRO* s. 5(1)(b), the Commissioner "may initiate an investigation of privacy compliance if there are reasonable grounds to believe that a person has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention."

[14] We began by investigating the apparent privacy breaches that resulted when the link to the Rankin School's camera feed was posted on Insecam.org. The CBC News story provided reasonable grounds to believe that the Board did not have reasonable security over the personal information on the video surveillance system, as required by *FOIPOP* s. 24(3).

[15] Our investigation revealed a lack of clarity around the authority to collect personal information by means of video surveillance, as required by *FOIPOP* s. 24(1). As a result, our investigation expanded to consider whether the collection by video surveillance was authorized.

1.3 Investigative process

[16] Upon initiation of this investigation our first step was to notify the Board of our intention to conduct this investigation. During that same initial contact, we discussed containment strategies with the Board, and confirmed that the passwords on the cameras had been changed.

[17] We conducted a site visit at the Rankin School and at the Board offices. There we viewed the surroundings, the video surveillance camera installation and interviewed the principal and IT staff in the presence of the Board's legal counsel. We reviewed relevant policy documentation provided by the Board.

[18] We reviewed the Insecam.org website to satisfy ourselves that the link to the camera feed from the Rankin School was no longer operational and to determine whether any further Nova Scotia school video surveillance feeds were available.

[19] On July 21, 2017, the Office of the Privacy Commissioner of Canada (OPC) wrote to the operators of Insecam.org, calling on them to immediately take down Canadian camera feeds which may contain personal information. The OPC copied our office on that letter.

[20] We interviewed the CBC News reporter who originally wrote the story revealing that the Rankin School video surveillance stream was available through the link on the Insecam.org website.

[21] We visited the camera manufacturers' website to view the manuals for each model of camera. We confirmed the security features available on the cameras, and the guidance the camera manufacturer provides for ensuring the protection of personal information gathered by the cameras.

[22] We sought and received technical assistance from our counterparts in the OPC and the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC). On our behalf, the OPC reviewed the technical specifications for the cameras to offer guidance on securing the specific devices. The specifics of that advice will be discussed in the analysis below.

[23] To better understand practices for video surveillance in schools, we interviewed representatives of every Nova Scotia school board. We met with Department of Education and Early Childhood Development officials and discussed video surveillance requirements, obligations and standards in Nova Scotia.

[24] We looked to other Canadian jurisdictions for their policies and practices around video surveillance in schools. Finally, we conducted a review of recent academic literature around efficacy and best practices with respect to video surveillance in schools around the world.

2.0 Issues

[25] The issues arising from this investigation are:

(1) Does the Board have reasonable security in place for the video surveillance system at Rankin School, within the meaning of *FOIPOP* s. 24(3)?
(2) Is the Board authorized, pursuant to *FOIPOP* s. 24(1), to collect personal information through video surveillance?

3.0 Analysis and Findings

3.1 Why is privacy important?

[26] *FOIPOP* defines personal information as "recorded information about an identifiable individual."[4] Nova Scotia Courts have interpreted this definition as "undeniably expansive," and have taken pains to make clear that the court should not interpret the definition restrictively.[5]

[27] The collection, use and disclosure of personal information by public bodies is limited to that which is authorized by *FOIPOP*. The purposes of *FOIPOP* include preventing the unauthorized collection, use or disclosure of personal information and protecting the privacy of individuals with respect to personal information about themselves held by public bodies.[6]

[4] *FOIPOP*, s. 3(1)(i).
[5] *Dickie v. NS (Department of Health)* 1999 NSCA 7239, at paras 30-34; *Sutherland v. Dept. of Community Services* 2013 NSSC 1, [*Sutherland*] para 25.
[6] *FOIPOP* s. 2(a)(iv) and 2(c).

[28] *FOIPOP* accomplishes these purposes by establishing rules to limit the collection, use and disclosure of personal information, as well as a rule to require reasonable security arrangements to protect personal information in the custody or control of the public body.[7]

[29] Almost thirty years ago, the Supreme Court of Canada noted the significance of privacy in supporting individual well-being and active involvement in a free and democratic society:

> [Privacy] is at the heart of liberty in a modern state. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[8]

[30] More recently, the Supreme Court of Canada commented on the expectation of privacy in public places, and the relationship between privacy and surveillance:

> It seems to me that privacy in relation to information includes at least three conceptually distinct although overlapping understandings of what privacy is. These are privacy as secrecy, privacy as control and privacy as anonymity…
>
> Anonymity permits individuals to act in public places but to preserve freedom from identification and surveillance…in a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the "situational landscape.[9]

3.2 Does the Board have reasonable security in place for the video surveillance system at Rankin School?

[31] Insecam.org functions as an aggregator for non-secured IP video surveillance cameras. It finds the IP addresses of video surveillance cameras that are linked directly to the internet. When the video feed from one of those cameras is viewable, Insecam.org publishes a link to the IP address on its site.

[32] It is important to note that Insecam.org does not stream live feeds of unsecured IP cameras; it merely provides links to them. The unsecured cameras exist independently, live streaming their content to the internet. Anyone with an internet connection and knowledge of the IP address can view the feed of an unsecured camera.

[33] During our investigation, Board officials gave the following reasons for the installation, purposes and security of the video surveillance system at the Rankin School.

---

[7] *FOIPOP* ss. 24, 26, and 27.
[8] *R. v. Dyment*, [1988] 2 SCR 417, 1988 CanLII 10 (SCC) at para. 17.
[9] *R. v. Spencer* [2014] 2 SCR 212, 2014 SCC 43, paras 38-44.

a. Installation

[34] In response to a request for records concerning the decision to install cameras, the Board provided the following context in its written submission dated July 25, 2017:

> There is a Design Requirements Manual for schools, which is produced in order to give suggestions for specifications for schools in the Province of Nova Scotia. In 2003, and perhaps earlier, the Design Requirements Manual for schools indicated that schools should be equipped with video surveillance. An excerpt from the Design Requirements Manual in 2007 is attached.[10]

[35] In the same submission, the Board points to a 2007 policy the Board adopted on security in schools. In support of its decision to install video surveillance cameras at Rankin School, the Board relies on a portion of the policy which states, "Where necessary, points of entry are to be provided with a video camera to monitor persons entering the building."[11] When this policy was subsequently revised in 2013, it maintained the same requirements for security cameras.[12]

[36] Rankin School was built in 2006-2007, and the Board initially decided not to install video surveillance at the school. The exterior cameras were added sometime after the school was built, but it is not clear when, exactly. The Board was unable to locate records of a decision to install the two exterior cameras. It notes that all records older than seven years have been destroyed.

[37] The camera pointed at the washroom entrance was installed in January 2015 in response to repeated incidents inside the washroom that involved a student. The installation of the washroom entrance camera occurred following a verbal agreement between the principal and the facilities coordinator. Prior to installing the washroom entrance camera, they discussed an alternative solution to the identified problem, installing a washroom for elementary school students, but settled instead on video surveillance. The Board recognized that it could not install a camera inside the washroom because it would be unreasonably privacy invasive, so it chose instead a camera pointed at the washroom's entrance. No explanation is given for why the other solution was rejected. No documentation was produced regarding that decision.

[38] The Board stated that all three cameras are operational 24 hours per day, 7 days per week.

b. Purposes

[39] The Board explained that it had a duty to protect students in the school, and that its video surveillance system was used for detection and deterrence of incidents. According to the Board, the cameras help ensure the security of students and staff and deter inappropriate behaviour. In the CBC News reports, the Board stated that the cameras were installed to prevent vandalism and property damage. In our interviews, the Board noted that this characterization oversimplified the

---

[10] In its submission the Board attached one page of the then Department of Transportation and Public Works' DTPW-DC350 Design Requirement Manual, Section 4 – Video Surveillance, 2007 Edition.

[11] Cape Breton-Victoria Regional School Board, "Policy and Administrative Procedures" - Security in Schools, Operational Services: 400, Policy Number: OST 430, Adoption Date: April 2, 2007 - Procedure 2(f).

[12] Cape Breton-Victoria Regional School Board, "Policy and Administrative Procedures" - Security In Schools & Administrative Buildings, Operational Services: 400, Policy Number: OST 430, Adoption Date April 2, 2007. Revised June 17, 2013 - Procedure 2(f).

risks, but did not dispute that prevention of vandalism or property damage was also a consideration.

[40] The Board stated that the cameras needed to be internet-enabled so that if a shooter entered the school, as happened in Columbine High School, police would be able to connect through the internet to the cameras and monitor the actions of the shooter in the school from their squad cars. The Board stated that schools in the Board that are larger than Rankin School provide a better example of this capability.

[41] The Board also noted that connectivity was important for technical support across the school board's large region. Since school staff review camera footage so infrequently, they often aren't able to get access to the video surveillance on their own.

c. Security of video surveillance system

[42] The washroom entrance camera was initially installed using only the default password. In a telephone conversation on May 4, 2017, Board staff advised OIPC investigators that between May 3 and the morning of May 4 the passwords to the cameras were changed. In correspondence received in September 2017, the Board's lawyer advised that the Board was alerted to the Insecam.org problem on May 2 and had changed the passwords before school began on May 3.

[43] The device that records and stores the footage at Rankin School is kept in the administration area, in a locked room. The administration and custodial staff have access to the physical space where the device is kept. The cameras themselves all have tamper-proof domes installed.

[44] The cameras are connected directly to the internet, the Board told us.

d. What is reasonable security?

[45] In Investigation Report IR16-02, I considered the meaning of reasonable security in the context of Nova Scotia's *Personal Health Information Act* (*PHIA*). In that report, I noted that every privacy statute in Canada incorporates the same or very similar language requiring "reasonable security" for the protection of personal information. Citizens reasonably expect that their personal information is being protected, regardless of the organization doing the collecting. Thus, I adopt the principles I articulated in IR16-02 and apply them here to *FOIPOP*'s s. 24(3) requirement that the head of a public body make reasonable security arrangements to protect personal information.

[46] In brief, the considerations underlying reasonable security are as follows:[13]

- Reasonable security is contextual. Overwhelmingly, what is clear in the case law is that reasonable security is intended to be an objective standard measured against the circumstances of each case.
- The more sensitive the information, the higher the security standard required.

[13] Investigation Report IR16-02, beginning at para 94.

- Reasonable security must take into account the foreseeability of the breach and the harm that would result if the breach occurred. The higher the risk of a breach, the higher the security standard will be.
- For public sector bodies, reasonable security also includes reasonable assurances to the public that the government is taking privacy protections seriously. Where government organizations hold personal information, the public has an increased level of trust that their personal information is being protected. This creates a high standard for government organizations to ensure security measures are in place.
- Industry standards and codes of practice can illuminate security requirements provided that following those practices reaches the contextual standards of reasonableness.
- The cost of implementing a new security measure may be a factor but it is on an extreme scale – reasonable security does not require a public body to ensure against a minute risk at great cost. A public body cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable security in another.
- Reasonable security applies to the entire life cycle of the records.
- The medium and format of the records will dictate the nature of the physical, technical and administrative safeguards.
- Procedures for establishing reasonable security must be documented, and organizations must be prepared to respond to the idea that employees won't always follow the documented procedures.

e. Security of video surveillance at Rankin School

[47] The breach came our attention on May 4, 2017, when CBC News published a story that the Rankin School video surveillance cameras were accessible through the Russian website. Six photographs, which the CBC News identified as screen captures from the school's video surveillance system, illustrated the story. Two of those images were from the camera pointed at the entrance to a washroom, three showed the parking lot and playground area, and one showed an entrance door. All images included a date and time stamp in the upper left corner. On the images of the washroom entrance, "change password" was clearly displayed in the upper left corner. The CBC News story did not make clear precisely how many cameras were accessible through the Russian website.

[48] During our site visit, we observed three cameras installed in Rankin School. The first was the fixed-mount camera across the hall from a washroom. The second was a camera at the entrance door, and the third was a pan-tilt-zoom camera on the corner of the building. This camera swept across the parking lot and playground.

[49] In our interviews on May 24 and 25, 2017, Board officials confirmed that the Russian website had included a direct link to its camera across from the washroom. The Board stated that this camera had a default password set by the manufacturer when it was installed. As soon as the Board learned this camera was streaming, the Board changed the password. The Board further confirmed that the exterior images that illustrated the CBC News story all came from Rankin School's two remaining video surveillance cameras.

[50] The Board refused to offer any suggestion as to how CBC News obtained images from the other two cameras. Instead it insisted that the only breach the Board was responsible for was the

first one – the camera streaming on the website. The Board insisted that the other two cameras had been password protected at the time, and therefore the Board had reasonable security in place to protect the personal information collected by the cameras.

[51] During our interview with the CBC News reporter, he explained that, once he had access to the washroom entrance camera through the Insecam.org site, he was able, with a very simple change of the numbering in the IP address, to access the other two cameras. The reporter confirmed that he was not prompted to enter a password to gain access to either of the other two cameras. Once he had changed a single number in the URL, he had access to the stream of the other cameras. He reported that he was even able to manipulate the one camera with pan-tilt-zoom capability.

The breach of the other two cameras

[52] Based on our security research, we concluded that when individuals accessed the Rankin School camera images, they were able to see the internet address or URL for the first camera. The labelling of that camera made it obvious that by changing the camera number at the end of the URL, a viewer might be able to see images from other Rankin School cameras if any existed. In some circumstances, once the camera URL is known, the fact that the other related cameras are password protected does not matter.[14] Users can access camera images despite not having passwords.

[53] With assistance from technical experts at the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia, the OIPC has determined that the Rankin School cameras were not secured against an "insecure direct object reference" vulnerability. In the world of technical security, this is a well-known vulnerability that results when one connected application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.

[54] In other words, any person who found the first camera while it was posted to Insecam.org and clicked through to view it, had the ability from that point to get around the password protection of the second and third cameras and view them by manipulating the publicly available URL of the first camera. Not only that, individuals who accessed the exterior pan-tilt-zoom camera were also able to manipulate the camera itself. As a result, all live feed images from all three cameras were available to users of the Insecam.org website up until sometime on May 3 or May 4, 2017.

[55] I began this discussion by listing some of the considerations that apply when determining whether or not a public body has made "reasonable security arrangements" to protect personal

[14] Breaches as a result of insecure direct object reference vulnerability are common and frequently find their way into the news. See, for instance: "Verizon patches serious email flaw that left millions exposed," https://threatpost.com/verizon-patches-serious-email-flaw-that-left-millions-exposed/118661/; "Uber portal leaked names, phone numbers, email addresses, unique identifiers," https://threatpost.com/uber-portal-leaked-names-phone-numbers-email-addresses-unique-identifiers/122128/; "Worldpay merchant portal allowed merchants to view customer card data, "https://www.scmagazineuk.com/worldpay-merchant-portal-allowed-merchants-to-view-customer-card-data/article/531699/, and "Citigroup hack exploited easy-to-detect web flaw," https://www.theregister.co.uk/2011/06/14/citigroup_website_hack_simple/.

information within the meaning of s. 24(3) of *FOIPOP*. Applying that criteria to the facts of this case I note:

- From an objective perspective, citizens would not normally expect that video surveillance images of children in a Nova Scotian school, near a washroom, in the hallways or on the playground would be available worldwide on the internet.
- In this case, the images included children, staff and visitors. Images of children as vulnerable citizens are of particular sensitivity.
- Changing manufacturer set passwords is a well-known and basic security step. In fact, the manufacturer of the washroom entrance camera advised users on screen to change the password.
- The insecure direct object reference vulnerability is a well-known vulnerability.
- The Board is in a position of trust with respect to children in its care. Where public bodies hold personal information, the public has an increased level of trust that their personal information is being protected and this creates a high standard for public bodies to ensure security measures are in place.

[56] Reasonable security, without a doubt, would require that video surveillance images of these children not be available through the internet. Further, the reasonable security requirement means that public bodies must be familiar with known vulnerabilities of technologies they choose to implement.

[57] **Finding #1:** I find that the Board failed to have reasonable security arrangements in place for all three video surveillance cameras at Rankin School at the time of the breach**.**

f. Were reasonable steps taken in response to the breach?

[58] When we evaluate the security of personal information following a privacy breach, we consider whether the public body followed best practices in managing the breach. These best practices are known as the "four key steps":[15]

1. Contain the breach
2. Evaluate the risks
3. Notification
4. Prevention

[15] This practice is articulated by the OIPC in our guidance document "Key Steps to Responding to Privacy Breaches," available on our website at https://foipop.ns.ca/. It follows the same approach other jurisdictions use. See, for instance: the Office of the Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches": https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf; the Office of the Information and Privacy Commissioner for British Columbia, "Privacy Breaches: Tools and Resources": https://www.oipc.bc.ca/guidance-documents/1428; the Office of the Information and Privacy Commissioner of Alberta, "Key Steps in Responding to Privacy Breaches" https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf; and the Office of the Information and Privacy Commissioner of Ontario, "Privacy Breach Protocol: Guidelines for Government Organizations": https://www.ipc.on.ca/wp-content/uploads/Resources/Privacy-Breach-e.pdf.

1. Contain the breach

[59] Within about a day of learning of the breach, the Board added a new password to the washroom entrance camera and so made the live feed at the URL unavailable to anyone without the appropriate credentials. Following the original link now leads to the message, "camera not available." The Insecam.org link to the Rankin School camera is now a dead link.

[60] The Insecam.org website originates from Russia. Its practice of streaming video surveillance was the subject of an investigation in 2014 by the Privacy Commissioner of Canada and six other privacy commissioners.[16] At that time, the six privacy commissioners wrote to the website operator calling on it to take down the site. The site did stop publishing links for a time but subsequently began listing a smaller number of camera feeds.[17] The Rankin School's video surveillance became one of the live streams available on Insecam.org sometime after the 2014 federal investigation.

[61] To confirm containment of the breach, OIPC staff independently reviewed the Russian website. Despite its claims of location accuracy being only "a few hundred miles," the Russian website provides precision location in tiny communities and on occasion to individual homes.[18]

[62] Based on this understanding of the precision of the website, we searched the Russian website's city list for a variety of place names that corresponded or potentially corresponded to the Rankin School. These included "Iona"; "Cape Breton"; "Narrows"; "Rankin"; "Barra Strait"; "Bras d'Or"; "Highland Village"; "Plaster Cove"; "Victoria"; "Baddeck"; Sydney"; and "Highway 223." This search returned no results for Rankin School.

[63] Based on the Russian website's disclaimer about the precision of the cameras being only a few hundred miles, we also widened our search to include Nova Scotia cameras generally. We estimate that the Russian website has links to at least 50 cameras based in Nova Scotia. We were unable to identify any others that, by their appearance, were the cameras at Rankin School.

[64] We performed a similar search on the "Wayback Machine" internet archive, also with no results reflecting the Rankin School.

[65] Later in our investigation, and at our request, the CBC News reporter provided us with the original link and IP address to the Rankin School camera from the Russian website. Contained in the link was a series of numbers that coincided with the IP address of the camera. We returned to Insecam.org and determined that the original link on the Russian website is no longer accessible. We also directly keyed in the IP address for the washroom entrance camera and were prompted to enter a username and password. We attempted to manipulate the URL and also

[16] Privacy Commissioner of Australia, Privacy Commissioner of Macao-China and the Information and Privacy Commissioners from Quebec, Alberta and British Columbia.

[17] The letter to operators of the webcam website is available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/let_141121/.

[18] For example, our research revealed video surveillance feeds from communities such as North River, PEI, population 5,000, Dalhousie, N.B., population 3,000 and Tusket, NS population 400. One video feed indicated that the city was actually a road in NS. Further investigation through Google Maps revealed that the feed was from an identifiable home on that road.

found that the remaining two cameras could no longer be streamed without entering a username and password.

[66] This search satisfied us that the immediate risk of further streaming had been contained.

[67] The Board stated that passwords for all video surveillance cameras, Board-wide, had been changed following the breach. It further stated that the new passwords followed password best practices. The Board had no written policy guidance on password practices.

[68] **Finding #2:** I find that the immediate causes of this breach have been contained.

2. Evaluate the risks

[69] The next step in appropriately managing a privacy breach is to evaluate the risks. In order to evaluate the risks associated with this incident, it is necessary to evaluate a number of factors including the nature of the personal information involved, the cause and extent of the breach and the foreseeable harm from the breach.

Personal information involved

[70] Due to the nature of the breach and its discovery, few other facts are known. During our interview with the Rankin School officials, they told us that the washroom entrance camera was installed sometime in January 2015 in response to a particular incident that occurred inside the washroom.[19] We don't know when, exactly, Insecam.org discovered this insecure camera. We don't know how long it was viewable to anyone with the IP address. We therefore don't know how many individuals' images were captured and streamed to the internet. We also don't know how many viewers took advantage of the insecure direct object reference vulnerability and viewed images from the other two Rankin School cameras.

[71] The first camera is located across the hall from the boys' washroom entrance in a primary to grade 12 school. Based on that location, in my view it is reasonable to assume that the cameras would have recorded images of identifiable boys and young men as they entered and exited the washroom. It is worth noting that a student at school in a moment of embarrassment, shame or other distress isn't presented with many options to hide away and be alone. Human nature, then, is often to retreat to a washroom, which provides some semblance of privacy. A camera that captures all of those moments has the potential to be recording highly sensitive personal information.

[72] The exterior school cameras would have captured images of children at play, and of children and likely their parents entering and exiting the school. Sometimes this will mean students leaving school sick, or otherwise departing for reasons they may have wished to keep to themselves.

[73] Because of the nature of the breach and the way in which it was discovered, we have almost no indication of precisely what personal information was involved. We know that the cameras are recording everything in their field of vision 24 hours a day, seven days a week. We

[19] During our interview, Board officials were uncertain of the installation date but later provided an invoice for the camera dated January 2015.

know that individuals would be identifiable in the records. We know that the school serves children from grades primary to 12, and employs staff including teachers, support staff and management staff. Volunteer staff and other visitors may also have been captured by the video surveillance.

[74] In my view, it is reasonable to assume that some of the personal information involved – students retreating to a washroom in distress; students leaving school sick – could be considered highly sensitive. Even where the information is routine, day-to-day activity in public view, the cumulative effect of video surveillance does reveal a great deal about individuals' personal lifestyle and habits.[20]

Cause and extent of the breach

[75] The immediate cause of the breach was the fact that the Board connected an IP camera directly to the internet and failed to properly password protect the camera. But this vulnerability exposed a second vulnerability – namely the insecure direct object reference.

[76] We have no information on when exactly the breach began. We do know that it can't have been before January 2015, which is when the washroom entrance camera was first installed. The individuals potentially affected by the breach include any students at the school, any staff of the school, and any parents who may have volunteered at or visited the school.

Foreseeable harm from the breach

[77] In my view, the main risks here are hurt, humiliation, damage to reputation or relationships, and social and relational harm. A link to the live stream of the Rankin School washroom entrance camera could be found directly on a website that has persisted in streaming video surveillance despite warnings from privacy commissioners from around the world. The link was viewable to anyone with a connection to the internet. Moreover, the other two cameras showing the entrance doors and the playground area were easily accessible through a basic and well-known security vulnerability. Neighbours and friends could have been watching out of simple curiosity or for more malicious purposes. Moreover, predators, the very people the Board asserts it is protecting the children from, may have been watching.

[78] The Board also must give consideration to its own reputation and leadership position as a custodian of student personal information. The Board stated that, in response to the notification letter that was sent out to parents, it received only five calls. Each of the callers was curious to better understand the breach, but was supportive and friendly. It is also worth noting that the CBC News' follow-up story quoted the parents of two students enrolled at Rankin as expressing concern about the breach, but also understanding and acceptance.[21]

[20] On this point, I echo the comments of my colleagues in British Columbia (Order P09-02) and Ontario (Privacy Complaint MC13-46).

[21] http://www.cbc.ca/news/canada/nova-scotia/privacy-commissioner-investigation-school-webcam-broadcast-1.4099658.

Risk assessment

[79] Because of the open-ended scope of the breach, the fact that the breach was a direct, live feed to the internet, and the potential for sensitive information to have been included in the live feed, I assess this privacy breach as being high risk.

3. Notification

[80] The third step in managing a privacy breach is to determine whether notification is appropriate and necessary. Nova Scotia's *FOIPOP* is badly outdated. One of its core deficiencies is that it does not mandate notification of affected individuals when a privacy breach occurs.[22] However, best practices across the country dictate it, especially where a breach is considered to be high risk.

[81] Notification conveys respect to the individuals whose privacy has been breached, and allows them to take steps to mitigate any potential harms.

[82] The Board provided us with a document entitled, "Provincial Privacy of Student Information Policy". It advised that its actions were guided by this document (provided by the Department of Education) including s. 5.1 which states, "school board shall have a privacy breach protocol that contains at minimum the requirements as outlined in Appendix B." Appendix B provides a very brief outline of the four key steps. The Board advised that it has not developed any breach protocol separate from this provincial policy document.

[83] In this case, the Board did notify all parents by letter that a breach occurred. It sent the letter home with every student at Rankin School. The Board provided us with a copy of the notification letter during our investigation. The letter is dated May 3, 2017, and states that the Board was alerted to the breach "earlier this morning." Immediate notification, as occurred in this case, is a best practice and I commend the Board for this prompt notification.

[84] My concerns with the notification are two-fold. First, it's not sufficiently specific about what happened. The notice states:

> [The Board] was notified that a breach of the security cameras at Rankin (School of the Narrows) had occurred. Following the notification the security breach was rectified and live feed from the cameras was stopped.

[85] Best practices call for the notification letter to be specific about precisely what was entailed by the "breach of the security cameras." It is insufficiently clear that the "live feed" of one camera was viewable by anyone who knew of the website that was streaming the feed and further, that the live feed was of a camera inside the school pointed at a boys' washroom entrance. The notification also failed to acknowledge that in fact, because of the indirect object

[22] The full discussion of the need to update Nova Scotia's access and privacy law is contained in the OIPC report, "Accountability for the Digital Age: Modernizing Nova Scotia's Access & Privacy Laws": https://foipop.ns.ca/sites/default/files/publications/annual-reports/Accountability%20for%20the%20Digital%20Age%20%28June%202017%29%20.pdf.

vulnerability, the school's other two cameras were also accessible by the public through the URL available on the Russian website.

[86] Second, the notification fails to advise individuals of their right to complain to my office about the privacy breach. In a small community such as that served by Rankin School, it may be easier for individuals who are not satisfied with the Board's response to complain confidentially to an independent oversight agency than directly to the school or the Board. In my view, the number of complaints to this office following a clear notification would be a more reasonable measure of parents' concern than direct calls to the school.

[87] **Finding #3:** I find that the Board's notification to parents was appropriately timely.

[88] **Finding #4:** I find that the Board's notification was lacking in appropriate specificity and detail.

[89] **Recommendation #1**:

a) I recommend that the Board develop its own privacy breach policy by January 31, 2018.
b) I recommend that the privacy breach policy include a requirement that notification consist of the following elements:
    - Date of breach
    - Description of breach
    - Description of personal information affected
    - Steps taken so far to control or reduce harm (containment)
    - Future steps planned to prevent further privacy breaches
    - Steps individuals can take – consider offering credit monitoring where appropriate
    - Information and Privacy Commissioner contact information – individuals have a right to complain to the Information and Privacy Commissioner for Nova Scotia
    - Board contact information – for further assistance

4. Prevention

[90] The final step in managing a breach is to develop strategies to prevent a future occurrence. Strategies should address both the immediate causes of the present breach and should improve the public body's ability to detect and manage future breaches.

[91] Typically, prevention strategies will address privacy controls in all of the following areas:

1. Physical controls
2. Technical controls
3. Administrative and personnel controls

[92] The Board's stated position was that, aside from making the initial changes to the technical controls (changing passwords), no further physical, technical, administrative or personnel control changes were required or made.

1. Physical controls

[93] The Board explained that the cameras record to a device that is locked in an on-site server room, accessible only to administration and custodial staff. The cameras themselves have tamper-proof domes.

2. Technical controls

[94] The fact that the cameras are linked directly to the internet presents significant concerns. Like "reasonable security" in the *FOIPOP* context, technical industry standards are flexible. There are "gold standards" and bare minimums that must be met. Reasonable security in these circumstances will lie somewhere between the two.

[95] One of the gold standards for securing IP cameras is that they are kept on local servers and/or secured behind a robust firewall. Even with a firewall, at a minimum, one long, strong, non-obvious password for the camera system is required.[23] The operator's manual for the washroom entrance camera provides, as its first recommended advice for network security: "Use this unit in a network secured by a firewall, etc." The other two manuals do not specifically address securing the devices behind firewalls, but they do appear to presume the cameras will be behind a firewall since they each recommend checking firewall settings as an early troubleshooting step.[24] One solution is to keep the cameras on a completely localized system, secure from the broader internet. In addition to a firewall, technical security experts recommend that each camera is protected by a long, non-obvious password.

[96] Another acceptable security practice is to ensure that user and host authentication functionality is activated. The cameras used by Rankin School have this capability.[25] The Board said that user authentication, enabling the cameras to ensure the usernames and passwords are properly set up, is now active. Host authentication limits the computers that will be allowed to access the camera by entering the IP address of the computer. Both should be active on the IP cameras should they remain connected directly to the internet.

[97] The Board stated that it was not aware whether the system allowed logging of user access to the cameras. The Board had not conducted any audits of user access to the cameras.

[98] Finally, the Board stated that passwords are alphanumeric and based on best practices. The Board stated that currently it has no written policy or standard to define acceptable passwords. The US Department of Commerce's National Institute of Standards and Technology (NIST) recently updated its guidance on password best practices. Among its recommendations are that technology itself sets password parameters of a minimum length of 8 characters, and allow maximums of up to 64 characters. Further, NIST recommends a large and comprehensive

---

[23] See, for instance: "12 Security Camera System Best Practices – Cyber Safe," available online at https://www.eagleeyenetworks.com/wp-content/uploads/2016/05/Eagle-Eye-Networks-12-Security-Camera-System-Best-Practices-Cyber-Safe.pdf; "Cisco Guide to Harden Cisco IOS Devices," https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html; "How to Secure Your IP Security Cameras," https://www.lifewire.com/secure-your-ip-security-cameras-2487488, and "How to Make Your Wireless Security Cameras Untouchable to Hackers," http://www.makeuseof.com/tag/make-wireless-security-cameras-untouchable-hackers/.

[24] Installation guides and owner's manuals for the three specific camera models at issue here.

[25] https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc47.

"black list" of unacceptable passwords, and allowances for all printable American Standard Code for Information Interchange characters and the space character.[26]

[99] Considering this range of possible technical controls against the reasonable security standards for the protection of personal information articulated above, I note the following:

- Sensitivity of information: The information the cameras record is highly privacy invasive, and potentially highly sensitive. This is especially the case with the camera recording the washroom entrance. This factor supports a high standard of security.
- Foreseeability and harm of a future breach demand a high standard of security:
    - A future breach or attempted breach is possible or even likely. The cameras have already been breached by a website that collects links to non-secured video surveillance cameras. The IP addresses remain the same. There is clearly an appetite on the internet to access what is connected but hidden.
    - A future breach of the video surveillance system would result in similar harms as this one. Those harms, as noted above, are high risk in my view.
- School Board reputation and leadership: The Board rightly points out its critical responsibility to protect the children in its care. Where, as in this case, surveillance footage of young children becomes viewable on the internet at large, this also means the potential for predators to be viewing the footage. In my view, this responsibility demands a high level of technical security.
- Industry standards: As noted above.
- Costs: We have no information on costs. Generally, IP cameras have been installed as the cost of those devices has come down. I would only note that insisting on cost efficiency through video surveillance but refusing to pay for the reasonable security of personal information implications of those devices is inconsistent with reasonable security standards across the country.
- Medium and format: These cameras provide real-time, live streaming video. Numerous risks arise in that context, and in my view, dictate a high level of reasonable security.
- Manufacturer support: Finally, one of the challenges with IP devices generally is that manufacturers stop supporting them after they have been on the market for a period of time. According to our research, the manufacturer of two of the cameras have stopped producing and pushing out firmware updates to fix security vulnerabilities.

[100] Considering all of these factors, it is my view that further work on technical security is required to protect against future privacy breaches.

[26] NIST Special Publication 800-63B, "Digital Identity Guidelines," available online at https://pages.nist.gov/800-63-3/sp800-63b.html#appA.

3. Administrative and personnel controls

[101] Administrative controls include policies on who can access the cameras, creating a reliable audit trail and an effective password policy. The Board states that currently the cameras have two levels of password access. There are "administration" passwords, which allow users only to access and view the camera feeds, and there are "operational" passwords, which allow users to access and manipulate the cameras, look at and recover stored footage, and view the live feeds.

[102] At Rankin School, the principal and vice-principal have administration passwords to view the video surveillance. In practice, the principal told us that all access to the cameras is done by the vice-principal.

[103] The Board told us that operational passwords are all held by staff at the Board's central offices. Three managers and ten technical support staff hold these credentials.

[104] The Board provided a copy of the staff confidentiality agreement which includes an undertaking to "access information in any and all files and electronic applications and databases only as required in the course of my duties, and … maintain the confidentiality of all such information." The policy from which this agreement is derived requires all staff to sign the confidentiality agreement, but includes no reference to any need for regular updates. Moreover, there is no indication in either the Board's literature or from our interviews that any audit logging or monitoring of system access takes place.

[105] The Board provided copies of the Provincial Privacy of Student Information Policy, prepared by the Department of Education and distributed to all school boards. It also provided the staff confidentiality policy. The Board stated that these are the documents that govern its privacy program. In my view, neither policy sufficiently addresses the Board's privacy responsibilities.

[106] **Finding #5:** I find that the Board has not yet implemented adequate technical or administrative controls to prevent a similar breach from occurring again.

[107] **Recommendation #2:** I recommend that the Board further secure its cameras either behind a firewall or by other equivalent technical strategy as approved by the OIPC by January 31, 2018.

[108] **Recommendation #3:** I recommend that the Board replace the two exterior cameras which are no longer supported by the manufacturer once it has completed a privacy impact assessment and ensured that the use of video surveillance is authorized (see Recommendation #7 below).

[109] **Recommendation #4:** I recommend that the Board update its policies and practices by January 31, 2018 to include:

a) Regular and recurring privacy training for staff;
b) Requirements to review and reaffirm confidentiality agreements annually;

c) An updated privacy policy that includes a requirement to log all access to video surveillance, including date, time, camera viewed and authorization;
d) A requirement that the Board's privacy officer conduct an audit of video surveillance access logs at least every six months;
e) Consistent with Recommendation #1, development of a Board-specific privacy breach policy;
f) A password policy that reflects industry-standard best practices, such as the NIST guidance.

3.3 Is the Board authorized to collect personal information through video surveillance?

[110] As we investigated the security issue, information arose that led us to question whether the Board is authorized to conduct video surveillance.

[111] A fundamental privacy principle is to limit the collection of personal information. After all, there is no risk of a privacy breach of personal information that has never been collected in the first place.

a. Video surveillance in Nova Scotia's schools

[112] Because we suspected that the Rankin School's video surveillance practices were likely consistent with or at least similar to the practices of other school boards in other parts of the province, as part of this investigation, we conducted a survey of all other school boards in Nova Scotia on their use of video surveillance.

[113] Currently, all school boards in Nova Scotia use video surveillance in their schools, with the earliest installations beginning over 15 years ago. One school board has a camera in every school. Results from the other school boards vary, but no school board told us they did not use video surveillance. The school boards provided a variety of responses to explain the purpose of their video surveillance programs. Those responses included preventing vandalism and other illegal activity, monitoring weather conditions and oil tanks, and most commonly, ensuring the safety of students and staff.

[114] Most school boards stated that no specific incidents led to the installation of cameras, but rather they were being used as precautionary or preventative measures. One school board informed us that installation is now a provincial design requirement for P3 (public-private partnership) schools throughout Nova Scotia. All school boards stated that the cameras were or could be monitored live, with all footage stored for a limited period. Three school boards have cameras that are web-enabled. Regarding access to the footage, specific staff were designated to view cameras and footage, but only two school boards stated that logs were kept regarding the number of times footage was used. Nearly all school boards had a policy in place for their surveillance programs, but none had completed a privacy impact assessment (PIA) on the privacy implications of video surveillance.

[115] The Department of Education's (Department) policy on school security planning promotes the use of Crime Prevention Through Environmental Design (CPTED).[27] According to

[27] "School Security Planning Guide," Nova Scotia Department of Education, March 2015.

the Department's policy, CPTED is considered to be the practical application of theories from environmental criminology that attempt to reduce crime in two ways. First, CPTED principles suggest environmental and building design approaches that reduce the opportunities and rewards of inappropriate behaviour. Second, those building approaches increase the risks of being caught doing inappropriate behaviour. CPTED building principles look for ways to increase "natural surveillance." At the same time, the policy incorporates video surveillance, including a requirement that cameras be positioned outside the entrances to washrooms.

[116] It is not clear precisely to whom this policy applies. In the scope section of the policy, the Department says that, "For the purposes of this project the contents of this document are requirements." However, in the preamble section on the same page, the policy states that, "this document … is not intended to be prescriptive in nature." The Department explained that "project" refers to individual school construction projects and would not apply to the Rankin School as it was constructed well before the policy came into force.

b. Why is the Board conducting video surveillance at Rankin School?

[117] In media reports, the Board stated that video surveillance was needed to prevent vandalism and damage to school property. In our interviews, the Board asserted that Board policy required a "video doorbell" to identify visitors to the school. Finally, the Board stated that video surveillance was necessary for the safety of staff and students and, in particular, that the Board needed the ability to provide police with "eyes in the school" in the event of an active shooter situation.

[118] The Board's told us that it installed video surveillance without conducting any privacy impact assessment.

c. When is collection of personal information through video surveillance authorized?[28]

[119] A public body, such as a school board, may only collect personal information in accordance with *FOIPOP* for one of three reasons:

1. Because it is expressly authorized by a statute.
2. Because it is collected for the purpose of law enforcement.
3. Because it is directly related to and necessary for an operating program or activity.

[120] I have previously noted that determining whether a collection of personal information was authorized first requires a two-step process to determine that a collection of personal information took place. The first question is whether there is any personal information; second, was there any collection of that information.[29]

[28] In conducting our investigation, we reviewed previous decisions from Canadian courts and information and privacy commissioners analyzing when the collection of personal information through video surveillance is authorized. A summary of those decisions can be found in Appendix 1 to this report.
[29] NS Review Report 16-06.

[121] *FOIPOP* defines personal information as "recorded information about an identifiable individual."[30] As Nova Scotia's Supreme Court pointed out in *Sutherland*, the definition is about an identifiable, not an identified, individual.[31]

[122] As I noted in Review Report 16-06, collection refers to a public body having obtained the personal information in the first instance[32] – that is gathered or acquired information.

[123] **Finding #6:** I find that the video surveillance cameras at Rankin School collect personal information as they capture, record and store individuals' images.

[124] Having determined that personal information is collected, I must now determine whether the school has authority to do so. The authorities to collect personal information under *FOIPOP* are given as follows:

> 24 (1) Personal information shall not be collected by or for a public body unless
> (a) the collection of that information is expressly authorized by or pursuant to an enactment;
> (b) that information is collected for the purpose of law enforcement; or
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

1. Collection expressly authorized by statute:

[125] British Columbia's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) mirrors Nova Scotia's. The collection authority in the BC *FIPPA* is found at s. 26. The first three provisions are substantially identical to *FOIPOP* s. 24(1). In 1998, then-Commissioner Flaherty conducted an investigation of the use of video surveillance by public bodies. At the time of that investigation, *FIPPA* s. 26 contained only the three provisions that we currently see in *FOIPOP*.

[126] Commissioner Flaherty, in the 1998 report, highlighted that the collection of personal information is restricted "to a defined set of circumstances," and went on to list them. The Commissioner noted:

> The legislation in question may expressly authorize the collection of personal information. Usually, however, the legislation will only give authority for a particular program, with only implied authority for the collection of personal information.[33]

---

[30] *FOIPOP*, s. 3(1)(i).
[31] *Sutherland.*
[32] Alberta Order P2006-008 determines that personal information is collected when a video camera records images. My predecessor in NS Review Report FI-09-40 also determined that video surveillance images qualify as personal information.
[33] BC OIPC Investigation Report P98-012.

[127] Subsequent to this investigation the BC OIPC developed "Public Sector Video Surveillance Guidelines" in 2001. Those have subsequently been updated in January 2014.[34] The BC video surveillance guidelines explain the meaning of "expressly authorized" thusly:

> Section 26(a) of FIPPA allows for the collection of personal information that is expressly authorized by statute. This is the most straightforward legal authority for collection. If there is a law that states that a public body is authorized to collect personal information using video or audio recording, then, so long as the collection is done in accordance with that law and for the specified purpose, it is authorized.

[128] In a 2000 decision, Commissioner Loukidelis' delegate was asked to determine whether the Insurance Corporation of British Columbia (ICBC) had "express authorization" to collect, among other things, the weight of an applicant for a driver's license. ICBC took the position that British Columbia's *Motor Vehicle Act* gave it broad powers to require the collection of personal information, including identifiers such as a license applicant's weight. Including multiple identifiers on the license helped to ensure that the license itself did serve as a genuine identifier of the holder.

[129] The commissioner's delegate noted that proof of identity was an important component of a driver's license once the license had been issued. He observed that including a driver's weight might have some embarrassment factor. But, he noted that the embarrassment factor could equally apply to many of the other identifiers collected by ICBC, and that if any collection that might cause embarrassment had to be ruled out, this would defeat the *Motor Vehicle Act'*s goal of providing proof of identification for licensed drivers. Finally, the delegate pointed out that general visual identifiers such as weight were a less privacy-invasive measure than other possibilities such as fingerprints or retinal images.

[130] The delegate considered the more restrictive approach the Office of the Information and Privacy Commissioner of Ontario (Ontario OIPC) had applied in considering its provision for express authorization. He noted the differences in the wording, and determined that applying a restrictive approach to *FIPPA* would undermine the statute's purposes.

[131] In determining that ICBC was expressly authorized to collect license applicants' weight, the delegate summed up the express authorization provision in BC's *FIPPA* as follows:

> It seems to me that the key protection offered by section 26 is that the collection of personal information be restricted to information that is reasonably related to the legitimate governmental purposes outlined in the section, and that it is not necessary to artificially restrict section 26(a) to the collection of specific types of information identified explicitly in legislation or delegated legislation.[35]

---

[34] BC OIPC guidance document, "Public Sector Video Surveillance Guidelines": https://www.oipc.bc.ca/guidance-documents/1601.

[35] Insurance Corp. of British Columbia, [2000] B.C.I.P.C.D. No. 15: https://www.oipc.bc.ca/decisions/133.

[132] In BC Order F-14-26, the adjudicator summarized the three other cases in which the BC OIPC set the outer bounds on this interpretation of "expressly authorized."[36] She pointed to Commissioner Loukidelis' 2007 report that determined a school board did not have express authorization to collect prospective employees' personal information through an online assessment tool because, while the school board had authority to hire staff, there was no express authorization to collect personal information to do so. The commissioner found that the implication that personal information would have to be collected for the hiring process insufficient for the requirements of s. 26(a).

[133] In Investigation Report F11-03, Commissioner Denham found that BC Hydro had express authorization to collect hourly readings of customers' electricity consumption through a smart meter. She based this interpretation on a provision in the regulations describing the capability of smart meters, which included a requirement that the smart meters be capable of recording "at least as frequently as in 60-minute intervals."

[134] Finally, in Investigation Report F12-01, Commissioner Denham considered ICBC's collection of digital photographs and biometric data from those photographs. She determined that the provision in the *Motor Vehicle Act* that required the license applicant to "submit to having their picture taken" was sufficient to be considered an express authorization.

[135] In support of the collection of personal information through video surveillance cameras in Nova Scotia, the Department of Education pointed to several provisions of the *Education Act*. That Act imposes a duty on teachers, principals, school board superintendents and school support staff to take reasonable steps to ensure that schools are safe and orderly and to attend to the safety of students. The *Education Act* also imposes a duty on school boards to promote its schools as safe, and to manage and keep safe all real and personal property.[37]

[136] The Board made no statement or argument that its video surveillance system was expressly authorized by statute.

[137] In my view, these provisions fall well short of expressly authorizing the collection of personal information through video surveillance. First, the requirements are worded in approximately the same way for a wide range of school board employees who have vastly different responsibilities vis-à-vis students. These are general duties and lack the specificity required to be considered an express authorization. Indeed, the obligation is clearly to take "all reasonable steps," leaving a wide measure of discretion for staff to determine what is reasonable in the circumstances. Such a level of discretion appears to run counter to an "express" authority.

[138] Second, there is only an implication that personal information will be collected. There are no express statements of the need to collect personal information to ensure student safety.

[139] Third, in contrast to the lack of specificity on collecting personal information so that teachers, principals, school boards and support staff can carry out their duties, I note the authority given to the minister to collect personal information. The *Education Act* gives the

---

[36] BC Order F14-26.
[37] *Education Act*, ss. 26(1)(k) and (n); s. 38(1)(e); s. 39(1)(g); s. 40(1)(c); s. 64(1)(f) and (ae).

minister explicit authority to "collect, directly and indirectly, and use personal information" for the minister's investigation and inspection responsibilities.[38] As Ruth Sullivan notes in *Statutory Interpretation*, "it is presumed that the legislature uses words and patterns of expression in a consistent way." She goes on to explain:

> The presumption of consistent expression applies not only to words and phrases but to any structure or feature of expression. Having done a thing once, the legislature is inclined to use the same or a comparable method when it sets out to do the same or a similar thing again. As this method is repeatedly used for a particular purpose, a convention is established. The more distinctive the convention, the more frequent the repetition, the more justified that this conclusion is always used to accomplish this purpose and any departure from it signals a different intent.[39]

[140] Given that the legislature expressly authorized the minister's collection of personal information but left the collection implicit when dealing with school staff, we must therefore assume that the legislature did not intend to make an express authorization for the collection of personal information for the *Education Act* provisions highlighted by the Department of Education.

[141] Fourth, an interpretation that the collection of personal information by video surveillance is not expressly authorized does not, on its own, frustrate the *Education Act*'s purposes of ensuring safe schools. This distinguishes it from the cases in BC where finding that the collection of the driver's weight was not authorized ran the risk of undermining the entire legislated function of the Department.

[142] Finally, in contrast to the general provisions in Nova Scotia's *Education Act*, I refer to the express authority given to school boards in BC to collect personal information through video surveillance. Section 74.01 of the BC *Schools Act*, provides as follows:

> 74.01 (1) A board may install and operate a video surveillance camera in a school facility or on school land for the purposes of protecting
>
> (a) the safety of individuals in a school facility or on school land,
>
> (b) an individual's belongings in a school facility or on school land, or
>
> (c) school property
>
> with the prior approval of the parents' advisory council for the school where the board proposes to install and operate a video surveillance camera.
>
> (2) A parents' advisory council may make recommendations to a board to install and operate a video surveillance camera in a school facility or on school land for the purposes set out in subsection (1).
>
> (3) If a board
>
> (a) has installed and operates a video surveillance camera in a school facility or on school land before the date this section comes into force, or

[38] *Education Act*, s. 141(kb).
[39] Sullivan, *Statutory Interpretation*, 2nd ed (Toronto, Ont: Irwin Law, 2007), pp. 167-168.

(b) installs and operates a video surveillance camera in a school facility or on school land for the purposes set out in subsection (1),

the board must conduct an annual review that assesses if the installation and operation of the video surveillance camera is accomplishing a purpose set out in subsection (1).

(4) Subsections (1) to (3) do not apply to the installation and operation of a video surveillance camera in a school facility or on school land on a temporary basis for a specific investigative purpose.

(5) Subsection (1) does not apply to a video surveillance camera installed in a school facility or on school land before the date this section comes into force.

[143] **Finding #7:** I find that the Board is not expressly authorized, within the meaning of *FOIPOP* s. 24(1)(a), to collect personal information by means of video surveillance.

2. Collection for law enforcement purposes

[144] *FOIPOP* s. 24(1)(b) states:

> Personal information shall not be collected by or for a public body unless … (b) that information is collected for the purpose of law enforcement;

[145] Neither the Board, the Department of Education, nor any other school board asserted that the Board has a law enforcement mandate, or that the collection is done for law enforcement purposes.

[146] Guidelines for video surveillance produced by other commissioners' offices have included guidance on interpreting the authority to collect personal information for law enforcement as follows:

> Information collected for policing purposes must be collected by a public body with a common law or statutory enforcement mandate. For example, it is not sufficient for a public body to claim an interest in reducing crime in order to justify collection for "law enforcement"; the public body must have authority to enforce those laws.
>
> In BC, the OIPC has determined in a number of Orders that an investigation must already be underway at the time the personal information is collected for s. 26(b) to apply. A public body is not authorized to collect personal information about citizens, in the absence of an investigation, on the chance it may be useful in a future investigation. Similarly, in order for a collection to be lawfully authorized as relating to a proceeding, the proceeding must be ongoing at the time of collection.[40]

[40] OIPC BC Public Sector Video Surveillance Guidelines, January 2014 at pp. 3-4 available at: https://www.oipc.bc.ca/guidance-documents/1601.

[147] The Ontario OIPC gives a similar interpretation:

> The institution must have a clear law enforcement mandate, ideally in the form of a statutory duty. As per the definition of "law enforcement" in section 2(1) of FIPPA and MFIPPA, this could be either with respect to "policing" or "investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings." Therefore, to justify the collection of personal information under this condition, it is not enough to claim a mere interest in policing or law enforcement investigations.[41]

[148] I agree with these assessments. Applying the requirements to this case, there is no evidence that the Board has a law enforcement mandate within the meaning of *FOIPOP* s. 24(1)(b).

[149] **Finding #8:** I find that *FOIPOP* s. 24(1)(b) does not authorize the Board to collect personal information through video surveillance.

3. Collection of information directly related to and necessary for an operating program

[150] The Board's position was that the video surveillance of students, staff and the public at the Rankin School was necessary for safety reasons. The *Education Act* creates and vests specific powers in school boards, superintendents, principals, teachers and support staff. The *Education Act* imposes a duty on each of these positions to, in a way that is consistent with their position and interaction with students, ensure that schools are safe for students. Safety of schools is mentioned in the preamble to the *Education Act*. I conclude from this that keeping schools safe is a critical part of the Board's operating program.[42]

[151] This means that, should the Board be able to demonstrate that video surveillance is directly related to and necessary for school safety, then collection of personal information through video surveillance could be authorized by *FOIPOP* s. 24(1)(c).

[152] The Board pointed to policy requirements as the source of authority for the installation of video surveillance.

[153] Design requirements for new construction of schools produced by the Department of Transportation and Infrastructure Renewal (TIR) have called for video surveillance to be installed at schools as far back as 2007.[43] The wording used in the policies appears to make video surveillance mandatory for all new construction and renovations.[44] This apparent requirement is true of the 2007 version of the design requirements that were in effect when Rankin School was built, it is true of the updated design requirements produced by TIR in 2010, and it is true of the Department of Education's *School Security Planning* document produced in 2015.

---

[41] Ontario IPC, Guidelines for the Use of Video Surveillance, October 2015 at page 5, available at: https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf.
[42] *Education Act*, ss. 26(1)(k) and (n); s. 38(1)(e); s. 39(1)(g); s. 40(1)(c); s. 64(1)(f) and (ae).
[43] Board representations, July 25, 2017
[44] DC350, Part 2, Educational Facilities Design Requirements: https://novascotia.ca/tran/works/dc350/Part2.pdf.

[154] However, witnesses from both the Departments of Education and TIR told us that both departments view the locations as suggestions, not requirements. There is no audit done to ensure schools are installing video cameras in the prescribed areas. Moreover, the explanation from the Board was that the first two exterior surveillance cameras at Rankin School were not installed during construction, but rather some time after.

[155] The Department of Education made clear to us that any discretionary installation of a video surveillance camera within existing construction and within a school board's budget was not subject to the design requirements.[45] In short, there were no specific policy requirements that expressly applied to the Board's installation of the washroom entrance camera in 2015. Further, it is unclear whether the 2007 Design Requirements applied to the Board's installation of the two exterior cameras, since the Board's told us that they were installed after the school had opened.

[156] I recognize that the Department of Education policy calls for video surveillance to be installed at every new school, and that each school board has implemented video surveillance in varying ways. I note that each school board is a public body under *FOIPOP*, responsible for making its own decisions on how the privacy rules will be implemented.

Directly related to

[157] Determining whether the collection of personal information is directly related to an operating program or activity requires a good understanding of what exactly the operating program or activity in question is. So, for example, when an employer collected reference information from a former employer of a job applicant without a job applicant's knowledge, this was determined to be "directly related" to an operating program, i.e. making a hiring decision.[46] Information related to whether an employee was accessing non-work related websites during hours for which he was being paid was determined to be "directly related to" an operating program, i.e. management of human resources. But information that revealed the employee's activities on the non-work related websites was determined not to be directly related to an operating program.[47]

Necessary for

[158] The second requirement of s. 24(1)(c) is that the information be "necessary" for the operating program or activity. As I have previously stated, under *FOIPOP* it is appropriate to hold public bodies to a fairly rigorous standard of necessity. I agree with the following criteria with respect to the use of the word "necessary" in *FOIPOP*:

- It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future.
- Nor is it enough that it would be merely convenient to have the information.
- The information need not be indispensable.

[45] Meeting with Department of Education, July 31, 2017.
[46] OIPC BC Order F14-26 at para 31. This reference check made without consent, was determined not to be "necessary" because the public body could simply have asked the applicant for further references (at para 48).
[47] OIPC BC Order F07-18 at paras 62-63.

- In assessing whether personal information is necessary one considers the sensitivity of the information, the particular purpose for the use, and the amount of personal information used in light of the purpose for use.
- *FOIPOP*'s privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection and use.[48]

[159] In media reports, the Board stated that video surveillance was needed to prevent vandalism and damage to school property. In our interviews, the Board asserted that Board policy required a "video doorbell" to identify visitors to the school. Finally, the Board stated that video surveillance was necessary for the safety of staff and students and, in particular, that the Board needed the ability to provide police with "eyes in the school" in the event of an active shooter situation.

[160] In practice, it is unclear how the camera system, as set up at the Rankin School, could provide any useful information in an emergency. Two of the three cameras are stationary. Two of the three cameras only provide views outside of the school.

[161] Moreover, academic research on the efficacy of video surveillance is, at best, mixed. When the Ontario OIPC conducted an investigation of the Toronto Transit Commission's video surveillance program in 2008, it conducted an examination of academic literature on the effectiveness of video surveillance, which the Ontario OIPC found wanting. The commissioner found few papers that didn't have some significant methodological flaw, and the resulting outcomes ran the gamut from video surveillance as a highly effective deterrent to crime, to video surveillance having no deterrent effect on crime. The one firm outcome was that the literature supports video surveillance as a useful tool for producing evidence that can be used to help investigate an incident after the incident has occurred.

[162] I commissioned a review of academic literature on the efficacy of video surveillance in schools and found that the research has not become much more definitive in the intervening years. Scholars observe that video surveillance provides schools with evidence that can be helpful in investigating an incident after it has occurred. But there is little support for the notion that they offer an effective prevention tool, despite claims that they are essential for protection.[49]

[163] In evaluating "necessity" public bodies should also consider the privacy invasiveness of the proposal and whether or not a less privacy invasive option is available. A significant collection of academic literature has arisen considering the impact that regular surveillance has on individuals. Scholars report that school children under constant video surveillance feel that video surveillance reflects a mistrust in them. When trust is undermined by video surveillance, it causes students to act as criminals or victims. Trust is replaced by unthinking obedience and discipline when under the gaze of the cameras.[50]

---

[48] A version of this list can be found in OIPC BC Decision F07-10.
[49] The OIPC commissioned an independent review of the academic literature around the effectiveness of video surveillance in schools. A summary of that review is attached as Appendix 2 to this report.
[50] See: Lotem Perry-Hazan and Michael Birnhack, "The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy, and Trust," *Cambridge Journal of Education*,

[164] Nova Scotia's Department of Education also acknowledges the potential negative impact of video surveillance in the *School Security Planning Guide*:

> A component of feeling safe while at school is absence of overt security measures that may create a belief that there is reason to be afraid. Oppressive security can also impart a message to building occupants that they are not trusted. This can in turn decrease the sense of attachment and engagement that is identified as essential for student achievement. A lack of student attachment and engagement is known to contribute to student crime and misbehaviour.[51]

[165] Bruce Schneier, in his book *Data and Goliath*, analyzed video surveillance against humanity's most primal instincts: "…[M]ammals in particular don't respond well to surveillance. We consider it a physical threat, because animals in the natural world are surveilled by predators. Surveillance makes us feel like prey, just as it makes the surveillors act like predators."[52]

[166] In discussing the use of video surveillance footage, the Board told us that the cameras have only ever been viewed after an incident has occurred. The cameras are not monitored at all. The two outdoor cameras have the ability to show who was arriving at the school and, particularly the camera pointing at the front door could function as a "video doorbell," allowing reception staff to know who was arriving before staff permit individuals to enter the school. But the video doorbell function is rendered superfluous by the fact that staff at the front desk can already see out the door, that the doors are locked at all times, and therefore the monitor is never actually used. The Board stated that the footage from this camera has never been viewed.

[167] Footage from the playground/parking lot camera was reviewed one time after an individual drove into the school's parking lot at night and did donuts with his or her car. The Board stated that it reviewed the footage, but was unable to discern anything helpful from it.

[168] The washroom entrance camera was installed in 2015 in response to a disciplinary issue. The Board felt it was necessary to monitor a student's access to the washroom, and settled on video surveillance as the means to do this. It said that the footage from the washroom entrance camera was reviewed one time to check on the disciplinary matter. The Board stated that the disciplinary issue in question was resolved very shortly after the camera was installed. The Board declined to provide any information to support its assertions that video surveillance was necessary to resolve the matter, or that correction of the issue was directly linked to video surveillance. Nor did the Board provide any explanation for why the washroom entrance camera continued to be in use after the resolution of the disciplinary issue.

---

http://www.tandfonline.com/doi/abs/10.1080/0305764X.2016.1224813; Lotem Perry-Hazan and Michael Birnhack, "Privacy, CCTV, and School Surveillance in the Shadow of Imagined Law," http://onlinelibrary.wiley.com/doi/10.1111/lasr.12202/full, and Bruce Schneier, *Data and Goliath*, WW Norton and Co., 2015.

[51] *School Security Planning Guide*, Nova Scotia Department of Education, March, 2015.

[52] See: Perry-Hazan and Birnhack, "The Hidden Human Rights Curriculum of Surveillance Cameras in Schools" Perry-Hazan and Birnhack, "Privacy, CCTV, and School Surveillance in the Shadow of Imagined Law," and Schneier, *Data and Goliath*.

[169] There is a distinction between the washroom entrance camera and the two exterior cameras. The washroom entrance camera was installed for a specific, identified purpose that was satisfied in 2015. The information we gathered with respect to the purposes for the exterior cameras is less certain.

[170] With respect to the washroom entrance camera, the operating activity at the time was the management of a disciplinary matter in relation to the use of the washroom. Whether or not the standards of s. 24(1)(c) of *FOIPOP* were met at the time of the installation is unclear, but there is no doubt that two years later, there is no active incident to investigate. Therefore, it cannot be said that the washroom entrance camera's collection of personal information is "directly related to" an operating program or activity. Further, there is no necessity for the washroom entrance camera within the meaning of s. 24(1)(c).

[171] Except in rare circumstances when there is very visible signage in place, private areas, such as washrooms and change rooms, should not be monitored by video surveillance. To do so would be inappropriate. Individuals have a much higher expectation of privacy in these spaces.[53]

[172] It is worth noting that the School Security Planning document lists "outside student washrooms" as one of the 'compulsory' camera locations. However, Department officials told us that these requirements are not mandatory. Even if they were, the Board would still have to establish that the requirements of *FOIPOP* had been met. It has not done so with respect to the washroom entrance camera.

[173] The use of video surveillance for managing individual incidents or issues may well be authorized by s. 24(1)(c) but once the incident is resolved, ongoing use will usually not be "necessary". In the absence of any explanation whatsoever of an ongoing issue relating to the washroom and given the highly sensitive nature of the information gathered by this camera, the camera should have been disabled immediately following the resolution of the incident in 2015.

[174] **Finding #9**: I find that the ongoing use of the washroom entrance camera is not authorized under s. 24 of *FOIPOP*.

[175] Because there is a lack of information regarding the specific purposes of the two exterior cameras and because, like all of the other school boards in Nova Scotia, the Cape Breton-Victoria Regional School Board has never conducted a privacy impact assessment of its video surveillance system, the best next step would be for the Board to undertake a proper privacy impact assessment of its video surveillance system. In conducting the privacy impact assessment, the Board should take into account best privacy practices including an evaluation of the implications of constant surveillance of children. The OIPC has published guidelines on the

[53] This position is consistently found in video surveillance guides and papers from around the world, for example BC's Public Sector Video Surveillance Guidelines, January 2014, https://www.oipc.ab.ca/media/556680/Guide_Video_Surveillance_Private_Sector_Mar2008.pdf and Alberta's "Guidelines for the Use of Video Surveillance", https://www.oipc.ab.ca/media/556680/Guide_Video_Surveillance_Private_Sector_Mar2008.pdf.

use of video surveillance that can help public bodies evaluate the pros and cons of video surveillance. The guidelines also provide practical guidance on how to implement video surveillance in a manner that respects privacy rights while still allowing the public body to address identified risks.[54]

[176] **Recommendation #5:** I recommend that the Board immediately disable the video surveillance camera located outside of the boy's washroom at the Rankin School.

[177] As noted above, we interviewed representatives of every other school board in the province and the Department of Education as part of this investigation. Given that all school boards in Nova Scotia are conducting video surveillance and none of them reported having completed a privacy impact assessment, I am sending a copy of this report to each school board under a separate cover. As part of the public education mandate of this office, the OIPC has offered to organize a joint privacy impact assessment workshop to bring together representatives from all of Nova Scotia's school boards. All of the school boards, except the Cape Breton-Victoria Regional School Board have agreed to participate in this workshop. We will conduct this workshop within the next four months.

[178] **Recommendation #6:** I recommend that the Board conduct a privacy impact assessment of its video surveillance system and provide the OIPC with a copy. The Board may either conduct the privacy impact assessment on its own, or send a representative to the privacy impact assessment workshop that the OIPC will conduct by January 31, 2018.

4.0 Summary of Findings and Recommendations

[179] **Finding #1:** I find that the Board failed to have reasonable security arrangements in place for all three video surveillance cameras at Rankin School at the time of the breach.

[180] **Finding #2:** I find that the immediate causes of this breach have been contained.

[181] **Finding #3:** I find that the Board's notification to parents was appropriately timely.

[182] **Finding #4:** I find that the Board's notification was lacking in appropriate specificity and detail.

[183] **Finding #5:** I find that the Board has not yet implemented adequate technical or administrative controls to prevent a similar breach from occurring again.

[184] **Finding #6:** I find that the video surveillance cameras at Rankin School collect personal information as they capture, record and store individuals' images.

[185] **Finding #7:** I find that the Board is not expressly authorized, within the meaning of *FOIPOP* s. 24(1)(a), to collect personal information by means of video surveillance.

[54] A copy of the OIPC's *Video Surveillance Guidelines* is available at: https://foipop.ns.ca/sites/default/files/publications/Video%20Surveillance%20Guidelines%20%2822%20June%202017%29.pdf.

[186] **Finding #8:** I find that *FOIPOP* s. 24(1)(b) does not authorize the Board to collect personal information through video surveillance.

[187] **Finding #9**: I find that the ongoing use of the washroom entrance camera is not authorized under s. 24 of *FOIPOP*.

[188] As a regular part of our investigation process, we provide public bodies with an advanced, embargoed copy of our investigation reports for two reasons. First, to confirm the factual accuracy of our findings and second, to obtain an advanced response to our recommendations. Typically, public bodies accept the recommendations and begin work on implementation before the report is published. This allows my office to report on progress within the investigation report itself. In this case, though we followed our usual practice of providing an embargoed copy of the report, the Board declined to respond preferring instead to receive the final version of this report.

[189] Therefore, consistent with s. 40 of the *Freedom of Information and Protection of Privacy Act*, the Board has 30 days in which to respond to these recommendations.

[190] **Recommendation #1**:

a) I recommend that the Board develop its own privacy breach policy by January 31, 2018.
b) I recommend that the privacy breach policy include a requirement that notification consist of the following elements:
    - Date of breach
    - Description of breach
    - Description of personal information affected
    - Steps taken so far to control or reduce harm (containment)
    - Future steps planned to prevent further privacy breaches
    - Steps individuals can take – consider offering credit monitoring where appropriate
    - Information and Privacy Commissioner contact information – individuals have a right to complain to the Information and Privacy Commissioner for Nova Scotia
    - Board contact information – for further assistance

[191] **Recommendation #2:** I recommend that the Board further secure its cameras either behind a firewall, or by other equivalent technical strategy as approved by the OIPC by January 31, 2018**.**

[192] **Recommendation #3:** I recommend that the Board replace the two exterior cameras which are no longer supported by the manufacturer once it has completed a privacy impact assessment and ensured that the use of video surveillance is authorized (see recommendation #7 below).

[193] **Recommendation #4:** I recommend that the Board update its policies and practices by January 31, 2018 to include:

a) Regular and recurring privacy training for staff;
b) Requirements to review and reaffirm confidentiality agreements annually;
c) An updated privacy policy that includes a requirement to log all access to video surveillance, including date, time, camera viewed and authorization;
d) A requirement that the Board's privacy officer conduct an audit of video surveillance access logs at least every six months;
e) Consistent with Recommendation #1, development of a Board-specific privacy breach policy;
f) A password policy that reflects industry-standard best practices, such as the NIST guidance.

[194] **Recommendation #5:** I recommend that the Board immediately disable the video surveillance camera located outside of the boy's washroom at the Rankin School.

[195] **Recommendation #6:** I recommend that the Board conduct a privacy impact assessment of its video surveillance system and provide the OIPC with a copy. The Board may either conduct the privacy impact assessment on its own, or send a representative to the privacy impact assessment workshop that the OIPC will conduct by January 31, 2018.

5.0 Conclusions

[196] In its preamble, the *Education Act* notes that "an orderly and safe learning environment where all students feel respected and accepted is a necessary condition for student success." No one disputes the importance of ensuring schools are safe. As much as they need to be safe, the *Education Act* also recognizes that students need to feel respected and accepted, and this is where the importance of effective privacy protections come into consideration.

[197] Privacy is fundamental to allowing individuals the space to grow, develop and live as autonomous and contributing members of a thriving democracy. Academic research on the effectiveness of video surveillance to be a proactive safety tool is, at best, mixed. But researchers are clear on the impacts video surveillance has on individual's sense of themselves: they negatively impact how trusted they feel, of how respected they feel and of how free they are.

[198] Moreover, video surveillance creates risks for school boards when they choose to implement it. Video surveillance collects a significant amount of information about an individual's lifestyle and habits and, if that information is not properly secured, has the potential to end up in the wrong hands and put to misuse.

[199] Because of its impacts on individuals' sense of autonomy, and of the risks video surveillance creates for school boards, it must be implemented only after thoughtful consideration of those privacy risks and impacts. I am optimistic that the recommendations in this report will lead to a more robust privacy program at the Board, and hopeful that it will spark a wider conversation around video surveillance in the province.

6.0 Acknowledgements

[200] I would like to thank the many public officials who cooperated with this investigation from the Department of Education, Department of Transportation and Infrastructure Renewal and from all of the school boards around the province. The purpose of these investigation reports is to ensure that any lessons to be learned from a privacy breach are shared for the benefit of Nova Scotians and for the education of all public bodies.

[201] The Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia both provided us with technical expertise for which I am grateful.

[202] I would also like to thank Robert Bay, Investigator, who lead this investigation and drafted this report.

October 12, 2017

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Appendix 1 – Overview of Recent Video Surveillance Cases

The collection of personal information through video surveillance has been addressed in a number of decisions from Canadian courts and information and privacy commissioners. In Canada, various jurisdictions have approached privacy regulation differently. Federally, we have the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) that applies to private-sector organizations. British Columbia and Alberta each have private sector privacy laws titled *Personal Information Protection Act* (*PIPA*). Each version of *PIPA* has been declared "substantially similar" to *PIPEDA*.

Every province has some version of *FOIPOP* governing the collection, use and disclosure of personal information by public bodies. A consideration of the tests for the collection of personal information by video surveillance under both types of statute demonstrates many common principles.

Private sector video surveillance authorities

One of the earliest reported decisions on collection of personal information by video surveillance is a 2001 case summary from the privacy commissioner of Canada under *PIPEDA*. In that decision, the commissioner found a private security company was not authorized to install full-time video surveillance monitoring of an intersection as a marketing demonstration of its capabilities. In completing his report, the privacy commissioner noted that video surveillance "must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law."[55]

In 2004, the Federal Court approved the installation of video surveillance to monitor the entrances and exits of a Canadian Pacific Railway (CP) maintenance facility. The Court approvingly cited the test developed by the privacy commissioner of Canada, and examined whether the video surveillance was necessary to meet a specific need; whether it was likely to be effective in meeting that need; whether the loss of privacy was proportional to the benefit gained, and; whether there was a less privacy-invasive way of achieving the same end.

CP was able to show to the Court's satisfaction that it had dealt with 148 incidents of theft, damage, trespass, vandalism and violence over five years. The surveillance was estimated to be effective based on a decline in those events following implementation of the video surveillance. CP advanced evidence that it had considered, but rejected as unfeasible, alternative means of deterring the problems. Finally, by pointing the cameras outside of work areas so only entrances and exits were captured, limiting the staff who could access the footage, and only viewing the footage after a report of an identified incident had occurred, CP demonstrated that it had minimized the privacy invasion to the extent authorized by the collection.[56]

The Alberta commissioner was asked to consider whether video surveillance installed inside a men's locker room at a fitness centre was authorized under *PIPA* in 2006. The fitness centre demonstrated that its members had suffered close to 900 thefts out of the lockers in a three-year

[55] Video surveillance activities in a public place, 2001 CanLII 21545 (PCC).
[56] Eastmond v. Canadian Pacific Railway, 2004 FC 852 (CanLII).

period. The fitness centre had attempted multiple different approaches to reduce the thefts, to no avail. The fitness centre demonstrated strict privacy controls over the video footage. The commissioner found that the fitness centre had demonstrated that a legitimate issue existed to be addressed through the collection of personal information; that the collection of personal information was shown to be effective in addressing the legitimate issue, and; that the collection of personal information was carried out in a reasonable manner.[57]

In 2009, the British Columbia OIPC found that a condominium corporation had exceeded its authority under *PIPA* to collect personal information by video surveillance. The adjudicator expressly contrasted the condominium corporation's stated need for video surveillance against the CP and Alberta fitness centre examples, noting that "the fitness club had 900 incidents and the rail yard 148 in less time than it took for Shoal Point to have fewer than ten."

The condominium showed that it had been subject to a break-in through an unmonitored door, that a stone bench had been damaged, and that the lift for disabled persons to use the pool was damaged through misuse. It asserted that it was concerned about resident safety and potential liability resulting from residents swimming in a pool that was just three feet deep. The adjudicator determined that this was not sufficient evidence for the level of video surveillance in place. He noted that the damage to the bench and lift were little more than normal wear and tear. He found that a live feed of the swimming pool was not justified on safety grounds since it could not be monitored at all times, and even if it could, the security staff would be unable to effect a rescue faster than by the less privacy invasive method of the emergency phone in the pool area. He dismissed the liability issue on the grounds that the condominium had warnings in place just like all the other condominium pool rooms in the area. The adjudicator accepted that video surveillance at the entry doors could be helpful to prevent break-ins, but that monitoring of those feeds should be restricted to the security desk.

The adjudicator concluded that the condominium had not shown a real need for the level of video surveillance that it had in place. He expressed concern at the way "function creep" had manifested, with the video surveillance being used to pursue bylaw infractions. He found that the condominium's arguments did not demonstrate reasonable expected benefits to those needs. Finally, he determined that the impact the condominium's video surveillance would have on privacy outweighed the stated benefits. The adjudicator accepted the collection of personal information through video surveillance to monitor entry doors, but rejected video surveillance of the condominium's pool and fitness centre.[58]

Public sector statutes

The private sector collection authority, considered above, is based on reasonableness. This distinguishes it from the public sector acts like *FOIPOP*, which sets out three specific circumstances under which collection of personal information is authorized. Under *FOIPOP*, collection may be permitted if it is expressly authorized by statute, if the collection is for law enforcement, or if the collection is directly related to and necessary for an operating program of a public body. When considering whether a collection is necessary, the tests developed under

[57] AB OIPC Order P2006-008.
[58] BC OIPC Order P09-02.

private sector legislation to determine reasonableness can help inform an analysis of what may be considered necessary.

There are limited case decisions on the collection of personal information through video surveillance. The use of video surveillance has been addressed in guidelines produced by several commissioner's offices, each of which has been helpful in drafting this report.[59] The Ontario OIPC has issued a number of decisions evaluating the collection of personal information by public bodies through video surveillance, and those also help inform this report. Their results are summarized below.

The authority to collect personal information in Ontario's public sector access and privacy law is worded somewhat differently than Nova Scotia's. The Ontario law states:

> 38(2) 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. R.S.O. 1990, c. F.31, s. 38 (2).[60]

In its first expansive consideration of the authority to collect through video surveillance, the Ontario OIPC considered a complaint about the implementation of a video surveillance system across the Toronto Transit Commission (TTC). The commissioner found there was no express authorization for the TTC to conduct video surveillance. However, since the TTC operated its own special constables, it was found to have a law enforcement role, and so video surveillance was authorized for those purposes. More broadly, the commissioner evaluated the TTC's operations to determine whether video surveillance was authorized for its proper administration.

The commissioner noted that it was an established principle that personal information merely being "helpful to have" was insufficient to meet the statute's requirement of "necessary." She then went on to observe that "safety and security are essential to the proper functioning of mass transportation systems." The commissioner noted that the breadth of a transit system limits the number of options for securing the system. She considered evidence of significant risk to transit operators, and the international climate of terrorist threats to transit systems. She examined reports of transit system security experts around the world who, relying on their experience with video surveillance systems, supported a video surveillance system as a means for ensuring the

---

[59] Office of the Information and Privacy Commissioner for Ontario, "Guidelines for the Use of Video Surveillance," October 2015: https://www.ipc.on.ca/wpcontent/uploads/Resources/2015_Guidelines_Surveillance.pdf; Office of the Information and Privacy Commissioner for British Columbia, "Guide to using overt video surveillance," December 2016, https://www.oipc.bc.ca/guidance-documents/2006; Office of the Information and Privacy Commissioner for Newfoundland and Labrador, "OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador," June 26, 2016, http://www.oipc.nl.ca/pdfs/GuidelinesForVideoSurveillance.pdf; "OIPC Guidelines for the use of video surveillance in schools," February 13, 2013, http://www.oipc.nl.ca/pdfs/SchoolGuidelinesVideoSurveillance.pdf; Office of the Saskatchewan Information and Privacy Commissioner, "Video Surveillance Guidelines for Public Bodies," March 2016, https://oipc.sk.ca/assets/video-surveillance-guidelines.pdf.

[60] Ontario *FIPPA*, s. 38(2).

transit system was safe. On the basis of this evidence, the commissioner concluded that the TTC's collection of personal information through video surveillance was authorized.[61]

An investigator with Ontario's OIPC applied similar principles to the video surveillance operation of a school in 2015. He noted that the operation of the school was clearly authorized by Ontario's *Education Act*, and that provisions of the *Education Act* that placed responsibility for student safety in the school's hands helped inform the necessity to keep the school safe. The investigator was satisfied that operating the school was authorized, and that keeping the school safe was a necessary part of the school's operation. He then turned to guidelines issued by the Ontario OIPC to help assess whether video surveillance was a necessary – as opposed to merely "helpful to have" – component of that safety. Those guidelines proposed the following considerations:

- 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;
    - 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.
- 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.

[61] *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report* - Privacy Investigation Report MC07-68.

The investigator saw evidence only of very limited numbers of incidents, and those incidents limited to altercations between students, drug use, theft and student pranks. In 5 of the 17 incidents, the video surveillance provided no helpful information to investigate. Finally, the investigator saw no evidence that the school board had taken steps to re-evaluate the need for and efficacy of the video surveillance system. In the end, he concluded that the school board had not demonstrated that its video surveillance program was necessary, or even necessary to the degree that it had been implemented. His recommendation was that the school board conduct a privacy impact assessment and make such adjustments as the PIA should produce.[62]

Very recently, the Office of the Saskatchewan Information and Privacy Commissioner completed an investigation into a privacy complaint filed by a City of Saskatoon (City) bus driver. The bus driver complained that the City had breached his privacy when it recorded his actions by video surveillance. The commissioner found that the City was authorized to collect personal information through video surveillance.[63]

I note that the Saskatchewan law has a very low collection standard:

> No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.[64]

This provision is distinguished from the collection authority in *FOIPOP* because it has no requirement that it be directly related to and no requirement that it be necessary for an operating program. There is limited application of the Saskatchewan decision in Nova Scotia.

[62] Ontario OIPC Privacy Complaint Report MC13-46.
[63] Office of the Saskatchewan Information and Privacy Commissioner Investigation Report 090-2017.
[64] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. L-27.1.

Appendix 2 – Summary of Academic Research on Effectiveness of Video Surveillance in Schools

To better understand the effectiveness of video surveillance in ensuring safety in schools, the OIPC commissioned a review of academic literature on the subject. That review is summarized in this appendix.[65] The review focused primarily on academic research conducted over the past five years specifically on surveillance in educational institutions.

Most of the academic literature reviewed laments the lack of quantitative and qualitative research on video surveillance in schools, arguing that most of the public support for video surveillance relies on perception of school safety and not actual safety.

For instance, a 2016 review of significant studies on the impact of school safety measures found broad support for the perception that video surveillance is among the most important safety measures by both students and school staff.[66] This finding was despite a 2011 paper that noted students had a clearer perception of the pervasiveness of video surveillance than their teachers, but were also more likely to feel that the cameras were not effective.[67]

Whatever the feelings of safety, academics struggle to define the effectiveness of video surveillance. The 2016 literature review that found high perceptions of safety found only one paper that evaluated the actual effects of video surveillance. That paper, itself limited in scope, determined that "security cameras had no effect on peer victimization."[68]

Researchers frequently consider the impact of peer victimization because "fear of victimization at school and school avoidance are correlated with negative academic outcomes."[69] One of the identified shortcomings of unmonitored video surveillance as a source of evidence in cases of student victimization is that it requires the victimized student or bystander to report the incident. Students report awareness of that shortcoming in unmonitored surveillance, and recognize that the culture of their school environments does not support reporting on peer behaviour, even if abusive.[70]

Other researchers have noted that video surveillance has a limited impact on deterring student misbehaviour because students simply relocate their misbehaviour. Students' awareness of video surveillance cameras does not necessarily cause them to desist from delinquent behaviour, rather

---

[65] Johnpaul Nwaezeigwe, "The efficacy and effects of CCTV cameras in schools: A research report," 2017.
[66] Jennifer M. Reingle Gonzalez, Katelyn K. Jetelina, Wesley G. Jennings, (2016) "Structural school safety measures, SROs, and school-related delinquent behavior and perceptions of safety: A state-of the-art review", Policing: An International Journal of Police Strategies & Management, Vol. 39 Issue: 3, pp.438-454, https://doi.org/10.1108/PIJPSM-05-2016-0065.
[67] Emmeline Taylor, "Awareness, understanding and experiences of CCTV amongst teachers and pupils in three UK schools," Information Polity 16 (2011) 303–318.
[68] Reingle, et. al., "Structural school safety measures."
[69] Fisher, B. W., & Tanner-Smith, E. (2016). Examining school security measures as moderators of the association between homophobic victimization and school avoidance. *Journal of School Violence, 15*(2), 234-257. doi:10.1080/15388220.2014.983644.
[70] Taylor, "Awareness, understanding and experiences of CCTV."

they simply conduct these actions in other areas where constant visual surveillance does not exist.[71]

A 2016 study on the effectiveness of video surveillance in reducing crime in universities found that the impact of video surveillance on violent and property crimes is not discernable once other control variables are factored. Further, video surveillance "at best augments other more effective and labor-intensive practices." The study questions the dominant view in popular discourse of video surveillance as a solution to crimes and delinquency. In reality, reducing crimes requires addressing problematic and embedded norms and behaviours among university students.[72]

Academics note as well that, regardless of the evidence for its efficacy, video surveillance continues to be a component of an increasingly pervasive school surveillance framework.[73]

The literature on the use of video surveillance in schools fails to present a definitive picture of the effectiveness of video surveillance in terms of school safety. This is probably due in part to the lack of substantial evaluations and statistics of video surveillance in schools with comparisons before and after their installation. Many scholars argue that such data is necessary to distinguish between perceptions of safety and actual safety.[74]

Another major problem highlighted in the literature review is the potential infeasibility of attempting to determine the impact of a single security measure, such as video surveillance on students, without considering the entire surveillance culture and framework that has permeated modern schools, as well as the sociological and psychological effects that it has on future generations.[75]

---

[71] Andrew Hope, (2015). Governmentality and the 'selling' of school surveillance devices. *The Sociological Review, 63*(4), 840-857. DOI 10.1111/1467-954X.12279, Association of Teachers and Lecturers (UK). (2013). "Use of CCTV surveillance in schools". URL (accessed 15 August 2017): https://www.atl.org.uk/policy-and-campaigns/policy-posts/use-cctv-surveillance-schools.

[72] Liedka, R. V., Meehan, A. J., & Lauer, T. W. (2016). "CCTV and campus crime." *Criminal Justice Policy Review,* 0887403416664947. DOI 10.1177/0887403416664947.

[73] Emmeline Taylor, "The rise of the surveillance school," *Routledge Handbook of Surveillance Studies,* 225, 2012 and Hope, "Governmentality and the 'selling' of school surveillance devices."

[74] Hope, "Governmentality and the 'selling' of school surveillance devices," and Taylor, "Awareness, understanding and experiences of CCTV."

[75] T.J. Servoss, (2017). School security and student misbehavior. *Youth & Society*, *49*(6), 755-778. DOI 10.1177/0044118X14561007. Also see Lotem Perry-Hazan and Michael Birnhack, (2016). The hidden human rights curriculum of surveillance cameras in schools: Due process, privacy and trust. *Cambridge Journal of Education,* 1-18. DOI: 10.1080/0305764X.2016.1224813, Emily Tanner-Smith, et. al., (2017). "Adding security, but subtracting safety? Exploring schools use of multiple visible security measures." *American Journal of Criminal Justice,* DOI: 10.1007/s12103-017-9409-3, and Emmeline Taylor, (2012). "The rise of the surveillance school." *Routledge Handbook of Surveillance Studies,* 225.

Bibliography

Advent IM Ltd, Senior Security Consultant (2012). "CCTV in Schools: Is surveillance in schools appropriate?" Retrieved 15 August 2017: <http://www.advent-im.co.uk/wp-content/uploads/2016/03/White-Paper-CCTV-in-Schools-v2.pdf>.

Association of Teachers and Lecturers (UK). (2013). "Use of CCTV surveillance in schools". Retrieved 15 August 2017: <https://www.atl.org.uk/policy-and-campaigns/policy-posts/use-cctv-surveillance-schools>.

Crawford, C., & Burns, R. (2016). "Reducing school violence: Considering school characteristics and the impacts of law enforcement, school security, and environmental factors." *Policing, 39*(3), 455-477. DOI: 10.1108/PIJPSM-05-2016-0061.

Fisher, B. W., & Tanner-Smith, E. (2016). "Examining school security measures as moderators of the association between homophobic victimization and school avoidance." *Journal of School Violence, 15*(2), 234-257. DOI: 10.1080/15388220.2014.983644.

Fussey, P. (2014). Emmeline Taylor, surveillance schools: Security, discipline and control in contemporary education. *Journal of Applied Security Research, 9*(4), 540-542. DOI 10.1080/19361610.2014.942832.

Hope, A. (2015). "Governmentality and the 'Selling' of School Surveillance Devices." *The Sociological Review, 63*(4), 840-857. doi:10.1111/1467-954X.12279.

Hope, A. (2016). "Biopower and school surveillance technologies 2.0." *British Journal of Sociology of Education, 37*(7), 885. doi:10.1080/01425692.2014.1001060.

Kids'N'Go. (2015). "CCTV at schools- Going Beyond Security?" Retrieved 15 August 2017: <http://www.kidsngo.org/cctv-at-schools-going-beyond-security/>.

Kupchik, A. *The Real School Safety Problem: The Long-Term Consequences of Harsh School Punishment.* (1st ed., pp. 101-117) University of California Press, 2016.

Liedka, R. V., Meehan, A. J., & Lauer, T. W. (2016). "CCTV and Campus Crime." *Criminal Justice Policy Review,* 0887403416664947. DOI:10.1177/0887403416664947.

Perry-Hazan, L., & Birnhack, M. (2016). "The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy and Trust." *Cambridge Journal of Education,* 1-18. DOI:10.1080/0305764X.2016.1224813.

Paton, G. (2014, April 20). "Classrooms put under 'permanent surveillance' by CCTV". *The Telegraph*. Retrieved 15 August 2017: <http://www.telegraph.co.uk/education/educationnews/10776060/Classrooms-put-under-permanent-surveillance-by-CCTV.html>.

Pickles, N. & Benbow S. (2012, September 12). "Is the use of CCTV cameras in schools out of hand?" *The Guardian*. Retrieved 15 August 2017: <https://www.theguardian.com/commentisfree/2012/sep/12/cctv-cameras-schools-out-of-hand>.

Reingle, J. M., Jetelina, K. K., & Jennings, W. G. (2016). "Structural school safety measures, SROs, and school-related delinquent behavior and perceptions of safety: A state-of-the-art review." *Policing, 39*(3), 438-454. DOI:10.1108/PIJPSM-05-2016-0065.

Servoss, T. J. (2017). "School Security and Student Misbehavior." *Youth & Society*, *49*(6), 755-778. DOI:10.1177/0044118X14561007.

Tanner-Smith, E., Fisher, B. W., Addington, L. A., & Gardella, J. H. (2017). Adding security, but subtracting safety? exploring schools use of multiple visible security measures. *American Journal of Criminal Justice*, DOI:10.1007/s12103-017-9409-3.

Tanner-Smith, E. E., & Fisher, B. W. (2016). "Visible School Security Measures and Student Academic Performance, Attendance, and Postsecondary Aspirations." *Journal of Youth and Adolescence, 45*(1), 195-210. DOI: http://dx.doi.org/10.1007/s10964-015-0265-5.

Taylor E. (2013, October 8) "School Surveillance Puts Trust at Risk", *Sydney Morning Herald*. Retrieved 12 August 2017: <http://www.smh.com.au/comment/school-surveillance-puts-trust-at-risk-20131007-2v494.html>.

Taylor, E. (2012). "The rise of the surveillance school." *Routledge Handbook of Surveillance Studies,* 225.

Taylor, E. (2010). "I spy with my little eye: The use of CCTV in schools and the impact on privacy." *The Sociological Review, 58*(3), 381-405. DOI:10.1111/j.1467-954X.2010.01930.x.

Taylor, E. (2017). "'This is not America': Cultural mythscapes, media representation and the anatomy of the Surveillance School in Australia." *Journal of Sociology*, *53*(2), 413-429. DOI:10.1177/1440783316667640.

Toronto District School Board. (2015). "School Safety and Engaged Communities". Retrieved 15 August 2017: <http://www.tdsb.on.ca/Portals/0/AboutUs/Accountability/SchoolSafetyEngagedCommunities.pdf>.

Webster, C. W. R., Töpfer, E., Klauser, F. R., Raab, C. D., & Taylor, E. (2011). "Awareness, Understanding and Experiences of CCTV Amongst Teachers and Pupils in Three UK Schools." *Information Polity: The International Journal of Government & Democracy in the Information Age, 16*(4), 303-318.