To: Boma Brown, CREAN

From: Michelle Liu and Olivia Startup

Re: The Legal Obligations of Private Organizations Regarding Surveillance Systems Capturing Sexual Assault

Date: April 12, 2021

You have asked us to research the legal landscape and treatment of surveillance footage in private establishments that could potentially capture a sexual assault.

Summary of Findings

The *Personal Information Protection Act* [SBC 2003] c 63 (the "*Act*"), which deals with the collection, use, and disclosure of personal information held by private organizations, is relevant for businesses that use surveillance systems. Although the *Act* does not explicitly include surveillance footage, the Office of the Information & Privacy Commissioner's *Guidance Document: Using Overt Video Surveillance*, (October 2017) ("OIPC Guide"), provides some insight as to the ways in which the *Act* is applicable to surveillance and offers recommendations as to how to comply with the *Act*. While the OIPC Guide is not a binding document, it does provide some insight as to how the OPIC might decide cases pertaining to surveillance footage.

Despite the crucial utility of surveillance footage as a form of evidence for sexual assaults, the OIPC has discouraged the increasingly prevalence of surveillance footage in private and public organizations and urges it should only be used as a last resort. Organizations are also left considerable discretion as to how they store and destroy footage, so long as it is reasonable. However, footage must be destroyed once it is no longer considered relevant for its intended purpose, and the OIPC recommends destruction after seven days, which could be very detrimental to sexual assault victims who do not report the incident immediately. Having access to such footage can often make or break a case; this is supported by recent research on the use of footage in investigating sexual offences.

While an individual has a right to a copy of video surveillance capturing their image, this right is likely impacted by privacy rights of other individuals captured on the footage. Two crucial exceptions to this are police seeking the footage in aid of an investigation and court orders demanding the footage. In the criminal context therefore, victims are largely at the mercy of the police taking the initiative to seek out the footage. In the civil context, an individual can apply to the court to order the footage; however, by this point in time, it is highly likely the footage will have been destroyed.

In light of these findings, better policy is required for high-risk locations such as nightclubs and bars as to the collection of surveillance footage and particularly the length of retention.

Background - The use of CCTV evidence in police investigations

Prevalence of sexual violence in public places

The majority of self-reported sexual offences occur in commercial or institutional establishments and private residences, and perpetrators are most commonly known to the victims (Stat Can, 2014). Roughly one in four of sexual assault victims reported that the incident occurred in a bar or restaurant. A 2018 Statistics Canada survey reported that one in three women 15-years and older experienced some form of unwanted sexual behavior in a public space in the 12 months prior to the survey. A fifth of women in London have reportedly been sexually assaulted while using public transport, and 90 percent of French women have been found to be victims of sexual harassment on public transport (Criado-Perez, 2019). Studies addressing sexual violence in India have echoed the finding that overwhelming percentages of women and girls feel unsafe in public spaces, specifically citing fear of sexual assault and harassment as being the most significant factor (Ceccato & Nalla, 2020). A study in Delhi found that nearly two in three women experience sexual harassment in public spaces, with over half citing public transport buses as one of the most common public spaces (Ceccato & Nalla citing Jagori & UN Women, 2011). Additionally, sexual violence that is not technically criminal is widespread and may guide how individuals perceive their safety in public spaces.

Usefulness of CCTV in investigating sexual assault

While studies indicate that the effectiveness of CCTV as a crime prevention tool is limited and that its use can displace crime (Lim & Wilcox, 2016), it appears effective at detecting criminal activity (Porter, 2009). Sexual violence occurring in public places has a greater chance of being subject to CCTV surveillance. Given that these are more likely to be stranger-on-stranger sexual assaults where no prior relationship exists, CCTV footage may be exceptionally important for investigative purposes.

This is supported by exploratory studies examining the usage of CCTV footage in criminal investigations. In a series of structured interviews of police investigators who had recently requested CCTV footage from Sydney's rail network, researchers found that assault investigators were most likely to rate footage as very useful, followed by investigators of sexual offences, with only four percent of sexual offence investigators rating the footage as not useful at all (Dowling et al., 2019).

A study analyzing crimes reported by the British Transport Police found that CCTV footage was classified as useful in 64.9 percent of crimes for which it was available (Ashby, 2017). In sexual offences, footage was classified as useful in approximately 80 percent of cases in which it was available. The probability of a crime being solved if CCTV was useful or not increased by 18 percent in sexual offence investigations.

Research has also shown that police requests for footage are associated with an increased likelihood of a matter being solved, particularly when footage was available and provided (Morgan & Dowling, 2019; Morgan & Coughlan, 2018).

Predictors of availability and usefulness

Successful retrieval of CCTV footage has been found to have a significant impact on the ability of police to solve crime, including sexual offences (Ashby). In over half of the cases examined, footage was not available when requested. Over five percent of these cases were due to the recording having been overwritten before it was retrieved. Retention rates of CCTV may

therefore be a predictor for availability (Ashby). Availability of footage is further impacted by the time at which it is requested by the police. Dowling et al found that one in three investigators submitted a request on the same as the incident or on the following day, but those investigating sexual offences were more likely to request footage more than one week after the incident.

Cases in which CCTV footage provided to police was assessed as being useful were more likely to be solved than cases where footage was assessed as not being useful (Ashby). This reflects the importance of well-designed systems and the barriers that can be encountered in using CCTV (Dowling et al). Usefulness may be limited by the number of public areas not covered by the range of the CCTV system; the quality of the footage, and visual obstructions. Ashby found that in cases where the CCTV was rated as not useful, 30.7% were due to insufficient quality of the footage. Sexual assault investigators may have more issues with image quality and physical obstacles obstructing their view (Dowling et al). This may reflect a deliberate commission of public sexual offences in environments that conceal their occurrence (Ceccato & Paz, 2017).

Footage quality may vary drastically depending on the number of cameras monitoring an area; the angles of the cameras; how they are mounted and whether they are static; their adaptability to reduced lighting; the number of frames per second, and whether the surveillance system uses analog or digital recording technology (Dowling et al).

The characteristics of the offence being investigated may further impact the usefulness of footage. Investigators of highly visible offences, i.e., those that involve violence, such as weapons offences, are more likely to find footage useful than investigators of 'covert' offences like burglary and theft. Depending on the nature of the sexual offence, it may fall in either of these two categories.

Where the footage does not capture the offence itself, it may capture relevant events surrounding the incident, aid in locating or confirming the identity of the suspect and corroborate statements. Studies on the specific efficacy of CCTV footage in sexual offence investigations is limited, but existing literature suggests that footage may serve different purposes. Dowling et al found that investigators of assault and sexual offences were most likely to report having used the footage to corroborate statements and to determine whether an offence had occurred.

Challenges

While the proliferation of publicly and privately-operated CCTV systems is predicted to play an increasingly greater role in investigations and in the courtroom, the efficacy of CCTV footage in prosecuting violent crimes, including sexual offences, is unclear. Possible issues include interpretation of unclear footage, and concerns with privacy and security.

Porter writes that the interpretation of visual narratives from CCTV images may present highly complex situations that are far from simplistic representations. Still, CCTV footage is increasingly interpreted as compelling evidence in court decisions. A study comparing intimate partner violence cases with digital photographic evidence and those without showed that digital evidence positively influenced case outcomes and led to more guilty pleas, higher conviction rates, and more severe sentences (Garcia, 2013). The same reasoning may be extended to the role of CCTV footage.

However, where image quality is low, unclear or otherwise unintelligible, police and prosecutors often turn to 'expert witnesses' to mediate or reinforce inculpatory interpretations. Edmond and Roque criticize that such witnesses may vary in substantial training and expertise, and question the potentially misplaced reliance on their interpretations of video evidence. Visual evidence can be unclear and open to alternative readings (Dodge, 2017), suggesting that interpretations may serve to strengthen as well as to attack a victim's case. Studies further caution that CCTV may itself serve as a locus of crime without adequate privacy safeguards. For instance, Ramirez & Lane (2019) found that surveillance systems may be used as a tool to exercise coercive control over victims. While there are positive implications for the use of CCTV, the quality of the images have significant impacts on its efficacy.

Analysis of the Law

Any violations of the *Act* must be brought to the OIPC Commissioner who can investigate, determine whether there have been any violations of the *Act*, and compel compliance with the *Act* through court order if necessary (s. 38).

There are some exceptions to the requirements of the *Act*. Section 3(2)(h) specifies that the provisions of the *Act* do not apply to "a document related to a prosecution if all proceedings related to the prosecution have not been completed." A document is defined to include "(a) a thing on or by which information is stored, and (b) a document in electronic or similar form" (s. 1).

We will address the specific provisions of the *Act* pertaining to the collection, use, and disclosure of personal information below.

The Collection of Personal Information

An organization must not collect, use or disclose personal information unless the individual gives consent or the Act authorizes it (s. 6). The Act defines "personal information" as "information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information" (s. 1). Although capturing someone's likeness or image is not explicitly referenced, the OIPC has treated audio and video surveillance recordings of individuals as personal information under the *Act* (see the OIPC Guide and Investigation Report P17-01; *British Columbia (Re)*, 2017 BCIPCD No 63 ("Investigation Report P17-01")).

An organization may only collect information that a reasonable person would consider appropriate in the circumstances and that fulfils the purposes as disclosed by the organization (s. 11). This requires a balancing of the interests of the organization in collecting the information and the privacy and self-autonomy interests of the individual, which the SCC has described as a fundamental value at the heart of democracy (paras 19-24 *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] SCJ No 62).

An organization is obligated to gain an individual's consent prior to collecting and using personal information (s. 6(1)). An individual provides explicit consent under ss.7(1) and 10(1) of

the *Act* when the organization provides written or verbal disclosure of the purpose for collecting the information and provides the position, name or title, and contact information for the individual designated to take questions about the collection. An individual can be deemed to give implied consent if, at the time the consent was allegedly deemed given, the purpose for collection would have been obvious to a reasonable person and the individual voluntarily provides their information (s.8(1)). Implicit consent may also be given if the organization provides the individual with notice of the collection and use of the information and provides the individual with sufficient time to reject the collection (s. 8(3)). The collection is limited to the stated or obvious "purpose." There are specified circumstances in which an organization may collect personal information about an individual without consent, including if it could reasonably be expected to "compromise the availability or the accuracy of the personal information and the collection is reasonable for an investigation or a proceeding" (s. 12(1)(c)) or if "the collection is required or authorized by law" (s. 12(1)(h)).

There is some conflicting case law as to whether s. 10, which outlines explicit consent, only applies to circumstances where an individual explicitly provides the information themselves. Order P12-01; *Schindler Elevator Corp (Re)*, 2012 BCIPCD No 25 held s. 10 only "applies to personal information where it is directly from the individual it is about, in consensual collections situations" (para 173). Commissioner Denham held this did not apply to information from a GPS system in employee vehicles. This reasoning was also applied in Order P12-01*; Kone Inc (Re)*, 2013 BCIPC 23 ("Order P12-01), which also dealt with tracking GPS information of employees. Alternatively, Order P09-02, *Shoal Point Strata Council (Re)*, 2009 BCIPCD No 34 ("Order P09-02"), the OIPC held s. 10 required a strata condominium to provide notice to all residents, owners, and visitors of a surveillance system. The OIPC Guide also indicates an organization is obligated to use adequate signage to notify the public that it is using a surveillance system. In light of the case law dealing directly with surveillance footage and the OIPC Guide, it is more likely than not that an organization will be required to notify the public. To comply with the *Act*, any signage must plainly indicate which areas are under video surveillance and for what purpose, for example: "This property is monitored by video surveillance for theft prevention." It must also provide contact information of someone in your organization for individuals to contact if they have questions about the surveillance. In Order P09-02, the OIPC held notification of the existence of security cameras without explaining their purpose does not meet the requirements for notification.

Organizations are also required to develop and follow policies and practices in order to comply with the obligations under the *Act* (s. 5(a)). The OIPC Guide specifically suggests developing a surveillance policy that contains:

- The rationale and purpose of the surveillance when and how monitoring and/or recording will be in effect;
- How recordings will be used;
- How long they will be kept;
- How they will be securely deleted; and,
- A process to follow if there is unauthorized access or disclosure.

Organizations should also periodically consider whether the surveillance is effective in addressing the problem it is meant to deal with, whether it is minimally invasive or if there are less privacy-intrusive ways to address the issue, and whether the problem still exists.

Order P09-01*; Cruz Ventures Ltd (cob Wild Coyote Club) (Re)*, 2009 BCIPCD No 16 ("Order P09-01"), offers some insight to the OIPC's approach to the reasonableness of an organization's collection of the personal information of customers. In this case, the OIPC held preventing minors from entering a club by scanning IDs of patrons and having their photo taken by the surveillance system was not a legitimate purpose because there was no evidence that entry by minors was "a prevalent, significant problem," or that the methods were effective in preventing the entry of minors (para 56). The commissioner also noted there were less privacy-intrusive means of achieving this goal. This case seems to suggest an organization might have to demonstrate a legitimate concern that sexual assaults were occurring within their establishment and that there was not a less privacy-intrusive means of capturing and preventing sexual assault. However, as noted in Order P12-01, the factors considered in Order P09-01 are not a strict test and must be considered within the context of each individual case to determine what was reasonable in the circumstances (paras 39-41). This case dealt with the collection and use of employee GPS information and the OIPC ultimately considered the following factors: the sensitivity of the information, the amount of personal information, the likelihood of effectiveness for the purposes of collection, the manner of collection and use of the personal information, less privacy-intrusive alternatives, and any other relevant factors (para 45). Commissioner Alexander ultimately held the collection was compliant with the *Act*, noting it was likely effective at verifying employee travel time and increasing efficiency, and it was not overly intrusive because the employer did not continuously monitor or review the information, nor did they collect information outside of working hours. Specifically, within the context of surveillance cameras, in Investigation Report P17-01, the OIPC noted "video surveillance should only be used as a last resort" (para 3). In Order P09-02, Commissioner Fedorak also considered the various locations of the cameras and distinguished his findings for surveillance cameras outside the building and in the parkade as opposed to inside the building in the pool area.

The OIPC Guide recommends that organizations limit the time surveillance is active and avoid unintended subjects. Examples of this include,

- Only turning on cameras for certain times of the day/night according to specific needs.
- Position cameras to capture least amount of information necessary (e.g. store security camera should not capture images of passersby on the street).
- Avoid areas where there is a heightened expectation of privacy.

The OIPC has not addressed the implications of surveillance footage in the context of preventing sexual assault.

The Retention and Destruction of Personal Information

The *Act* also includes some provisions on how personal information is to be retained. Per s. 34, "An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks." The OIPC Guide recommends storing recorded images in a secure location, not removing the recording from the premises, and following a secure storage protocol. The OIPC also advises there be limited access to the footage only to authorized individuals. Authorized individuals should only review the recorded images to investigate a significant security or safety incident, such as criminal activity. This principle was

demonstrated in Order P09-02, in which a strata condominium implemented a video surveillance in the building to prevent unauthorized entry, theft, or a threat to personal safety or damage to property. The OIPC held the *Act* did not permit a strata condominium to routinely review each day's footage in the absence of a complaint or evidence of unauthorized entry, etc.

"If an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it" (s. 35(1)). We were unable to find the application of this provision in a customer context, so it is unclear whether an organization submitting surveillance footage of a sexual assault requires organizations to keep the footage for a year. Based on a plain reading of the text however, this would presumably be captured by s. 35(1).

Finally, an organization must destroy its documents of personal information as soon as it is reasonable to assume that (a) "the purpose for which that personal information was collected is no longer being served by retention of the personal information," and (b) "retention is no longer necessary for legal or business purposes" (s. 35(2). The OIPC Guide recommends preparing a retention and destruction schedule outlining when and how footage will be destroyed.

Since the OIPC recommends retaining the footage no longer than seven days, and victims do not always report sexual assaults within seven days or the police may not investigate within seven days, it is possible important evidence is frequently destroyed prior to any requests or demand of the footage. This will ultimately depend on a company's discretion as to when it will destroy the footage, but it is unlikely organizations will have long retention policies. Storage capacity can be costly, and expenses will further vary depending on quality of the footage. For example, in a nightclub open for five hours per night, three days per week, over 52 weeks, this results in 780 hours of footage per year that must be stored. Therefore, clear directives are likely required to incentivize or compel longer retention of footage.

The Disclosure of Personal Information

An organization's use of the footage could also be influenced by the right of individuals to request access to their personal information (s. 23(1)). The OPIC Guide states organizations should be prepared to provide a copy of the relevant footage upon request. However, there are certain circumstances in which an organization is not permitted to disclose the information, and certain circumstances where it has the discretion to refuse disclosure.

An organization must not disclose personal information in the following circumstances:

(a) if disclosure "could reasonably be expected to threaten the safety or physical or mental health of" another individual

(b) if disclosure could cause immediate or grave harm to the individual who made the request; and

(c) if disclosure "would reveal personal information about another individual"

(s. 23(4))

While s. 23(4)(c) raises some concerns on the ability of an organization to release footage that contains the identifiable images of employees or other non-related individuals, the personal information protected under this provision "must be reasonably capable of identifying a particular individual either alone or when combined with information from other available sources" (para 22 Order P20-01; *Canada Life (Re),* 2020 BCIPC 6). There have been cases in which the OIPC found redacted documents complied with this provision (see Order P14-03; *Canadian Forest Products Ltd (Re),* 2014 BCIPCD No 49). An organization could then presumably comply with this provision by blocking out the faces of any non-related individuals. They may also be obligated to conceal the identity of the accused in this case, which would defeat the purpose of requesting the footage. However, just asking for the footage could arguably put the organization on notice that it should hand the footage over to the police or in the very least retain the footage longer. In order to make a request, an individual simply needs to submit the request in writing with sufficient detail for the organization to be able to identify the information sought (s. 27), and an organization must respond within 30 days (s. 29).

There are also some circumstances in which an organization has the discretion to decide whether or not to disclose the information to an individual, including if "the information was collected or disclosed without consent, as allowed under s. 12 (see above) or s. 18 (see below), for the purposes of an investigation and the investigation and associated proceedings and appeals have not been completed" (s. 23(3)(c)). An organization may also refuse to confirm or deny the existence of personal information collected as part of an investigation (s. 30(2)).

While disclosure is generally only permissible with consent, there are specified circumstances under which disclosure without consent is permitted. An organization is entitled to disclose information in the following circumstances:

> (c) it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for the purposes related to an investigation or proceeding
> (i) the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court
> (j) the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation,
>
> (i) to determine whether the offence has taken place, or
> (ii) to prepare for the laying of a charge or the prosecution of the offence
>
> (s. 18(1))

Therefore, while any employees or other individuals captured on the surveillance footage could impact the ability for a victim to demand the footage themselves, s. 18(1)(j) nonetheless gives an organization the right to disclose the footage to police without the consent of the individuals in the event of it capturing a sexual assault. In the event the police have not sought out the footage however, it is potentially much more difficult for a victim of sexual assault to access the footage if it conflicts with another individual's privacy rights. Furthermore, in a criminal proceeding, the application for a court order or subpoena of the footage would be entirely in the hands of the police or Crown counsel.

In the context of civil proceedings, per Rule 7-1(18) of the *Supreme Court Civil Rules*, BC Reg 168/2009, the court can bring notice to third parties to a dispute for documents in their possession. This must be done on an application under Rule 8-1, which includes summarizing the factual basis for the application, setting out any legal authority for the order sought (Rule 8-1(4). This application must be served on all relevant parties, including any other person who may be affected by the order sought (Rule 8-1(7). In this case, the victim has considerably more agency in compelling the court to order the evidence. A problem with this process however, is that civil proceedings for sexual assault are likely to occur after criminal proceedings have proven fruitless. By that time, it is highly likely any relevant footage will have been destroyed.

Finally, the use of the footage as evidence will be subject to several factors. In *R v Nikolovski*, [1996] SCJ No 122, 3 SCR 1197, the store surveillance camera was used to identify and convict the accused of robbery. The court held the weight to be afforded to video evidence will be assessed by the clarity and quality of the footage, the length of time the accused appears on the footage, and whether or not the video has been altered. The court upheld that this could be used as the sole piece of evidence identifying an accused.

Survey of Businesses and Police Departments

We contacted 46 private businesses in Victoria and Vancouver, and 16 police departments in BC to ascertain their internal policies and experiences relating to surveillance footage. We received responses from six businesses: one which stated that they did not have any surveillance systems, and two which expressly declined to participate. We received one police department response.

We asked the following questions of the businesses:

- Do you have security cameras or CCTV set up in your establishment?
- If so, what is your policy on how long the footage is to be stored?
- Is your surveillance system installed indoors or does it capture the street outside your establishment as well?
- In what manner is the footage stored?
- What is the process if the police request access to your footage?
- What is your policy on dealing with this footage if you believe it has captured a crime, particularly sexual assault?
- In your experience, have policies with respect to your surveillance system posed practical issues in the event a review of that footage is required?
- Does the organization have procedures to respond to questions about their policies and practices? Has the organization assigned an individual to monitor compliance with the *Personal Information Protection Act*?

We asked the police departments the following questions:

- What is the typical process if your police department believes a sexual assault may have been captured by surveillance footage in a private establishment?
- Have you faced any barriers to obtaining this type of footage?

- How long does this process usually take?

Summary of responses

Of the private businesses that had surveillance systems, none indicated having an explicit policy on the collection and storage of surveillance footage. One business expressly stated that they did not have any policies on the storage of footage. Conversely, all the private businesses that had surveillance systems recalled previous police requests for footage, but none had experienced requests for sexual assault investigations. Despite being similar types of establishments, retention lengths of footage varied between 48 hours and six weeks. There was further variation in whether the business had indoor surveillance, street-level surveillance, or both. According to the Vancouver Police Department, the process of obtaining surveillance footage is governed by search and seizure laws. However, the length of this process can vary drastically depending on the circumstances of each investigation.

Limitations of the Survey

Due to many temporary closures in response to COVID-19 health measures, we unfortunately received a very limited response. In addition, many businesses appeared reluctant to participate or were unsure about how to direct our inquiry. For bars and restaurants, it was difficult to find a time when the manager was on location and had the time to answer any questions. Emails sent in response largely went unanswered. While limited, the responses highlight a lack of consistency between private establishments in managing surveillance footage and its likely detrimental effect on victims' cases.

See attached Appendix A for the detailed responses from the survey.

Conclusion

The *Act* requires an organization not to collect, use, or disclose personal information without the consent of individuals, which would include surveillance footage capturing an individual's likeness. However, an individual will be deemed to have given implied consent if the organization provides proper notice of the collection and the purposes of collecting the information. An organization is permitted to collect information without an individual's consent if it would compromise the availability or accuracy of information used for an investigation or proceeding.

While the *Act* explicitly requires organizations to develop policies for the collection, retention, security, and destruction of personal information, the legislation leaves a lot of discretion to organizations to determine the content of those policies. An organization may only collect information that a reasonable person would consider appropriate in the circumstances and that fulfils the purposes as disclosed by the organization. The OIPC uses the 'reasonable person test' to decide whether an organization has carried out its responsibilities for the collection, use, and disclosure of personal information under *PIPA*. What is reasonable will depend on the facts of each case; however, the OIPC has typically considered whether the purpose for the collection of personal information is reasonably justified, whether it affects the issue the organization is seeking to address, and whether there were less privacy-invasive alternatives. For businesses

using surveillance systems, they will have to post a notice upon entry warning of the surveillance system and its purposes.

Organizations are also obligated to keep personal information secure and to limit access to the information and only review it when necessary. The OIPC Guide recommends organizations to limit the amount of time that surveillance is active, and to keep retention length of video footage to a maximum of seven days. However, if the footage has been used to make a decision about an individual, it must be retained for at least one year after using it.

On an individual's request, organizations should be prepared to provide a copy of the relevant footage. However, if the information was collected without consent in compliance with the act and is for the purposes of an ongoing investigation, disclosure of the footage upon an individual's request is discretionary. Disclosure upon request is not permitted if it would put the individual or someone else in danger or if it would reveal the personal information of another individual. Disclosure without an individual's consent is also permissible if it is provided to law enforcement to aid in an investigation. Therefore, while capturing an employee on surveillance footage could impact an organization's use and disclosure of the footage, it would nonetheless be able to provide the footage to the police without the consent of the employee.

While this footage can be crucial evidence in sexual assault cases and can even be used as the sole evidence identifying the defendant, there are a number of limitations that can prevent a victim from being able to utilize it. The footage must clearly identify the defendant and demonstrate the sexual assault in order for it to be viable evidence. Current OIPC recommendations also encourage short retention of any surveillance footage, which could be detrimental to a victim if the footage is not sought immediately after the assault occurs. Private establishments are not mandated to install surveillance systems, including for potentially high-risk places like bars and clubs. Finally, in criminal proceedings, the victim is left to the police and Crown counsel's discretion as to whether they will pursue the footage. While the victim has more agency in civil proceedings to request a court order of the footage, the timeline of civil proceedings makes it likely that the footage will have been destroyed.

Sources Consulted

Legislation

Freedom of Information and Protection of Privacy Act, [RSBC 1996] c 165

Personal Information Protection Act, [SBC 2003] c 63

Supreme Court Civil Rules, BC Reg 168/2009

Jurisprudence

Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62, [2013] SCJ No 62

Investigation Report P17-01; *British Columbia (Re)*, 2017 BCIPC 58

Order P09-01*; Cruz Ventures Ltd (cob Wild Coyote Club) (Re)*, 2009 BCIPCD No 16

Order P09-02, *Shoal Point Strata Council (Re)*, 2009 BCIPCD No 34

Order P12-01*; Kone Inc (Re)*, 2013 BCIPC 23

Order P12-01; *Schindler Elevator Corp (Re)*, 2012 BCIPCD No 25

Order P14-03; *Canadian Forest Products Ltd (Re)*, 2014 BCIPCD No 49

Order P-20-01; *Canada Life (Re)*, 2020 BCIPC 6

Secondary Sources

Alexa Dodge, "The digital witness: The role of digital evidence in criminal justice responses to sexual violence" (2017) 19:3 Feminist Theory 303 online: Sage Journals https://journals.sagepub.com/doi/10.1177/1464700117743049>

Anthony Morgan & Christopher Dowling, "Does CCTV help police solve crime?" (2019) No 576 Trends & issues in crime and criminal justice, online: AIC <https://www.aic.gov.au/publications/tandi/tandi576>

Anthony Morgan & Maggie Coughlan, "Police use of CCTV on the rail network" (2018) No 561Trends & issues in crime and criminal justice, online: AIC <https://www.aic.gov.au/publications/tandi/tandi561>

Caroline Criado-Perez, Invisible Women (New York: Abrams, 2019) at 49-55

Christopher Dowling et al, "How do police use CCTV footage in criminal investigations?" (2019) No 575 Trends & issues in crime and criminal justice, online: AIC <https://www.aic.gov.au/publications/tandi/tandi575>

Fanny A Ramirez & Jeffrey Lane, "Communication Privacy Management and Digital Evidence in an Intimate Partner Violence Case" (2019) 13 International Journal of Communication 5140.

Glenn Porter, "CCTV images as evidence" (2009) 41:1 Australian Journal of Forensic Sciences 11, online: Taylor & Francis <https://www.tandfonline.com/doi/abs/10.1080/00450610802537960>

Hyungjin Lim & Pamela Wilcox, "Crime-Reduction Effects of Open-street CCTV: Conditionality Considerations" (2016) 34:4 Justice Quarterly 597, online: Taylor & Francis <https://www.tandfonline.com/doi/abs/10.1080/07418825.2016.1194449>

Jagori & UN Women, Safe Cities Free of Violence Against Women and Girls Initiative: Report of the Baseline Survey Delhi 2010 (New Delhi: Jagori & UN Women, 2011), online:

Jagori <http://www.jagori.org/wp-content/uploads/2011/03/Baseline-Survey_layout_for-Print_12_03_2011.pdf>

Matthew P.J. Ashby, "The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis" (2017) 23 Eur J Crim Policy Res 441, online: Springer <https://link.springer.com/article/10.1007/s10610-017-9341-6>

Shana Conroy & Adam Cotter, "Self-reported sexual assault in Canada, 2014" (2017), online: Statistics Canada <https://www150.statcan.gc.ca/n1/pub/85-002 x/2017001/article/14842-eng.htm>

Vania Ceccato & Mahesh Nalla, Crime and Fear in Public Places, 1st ed (London: Routledge, 2020)

Vania Ceccato & Yuri Pax, "Crime in Sao Paulo's metro system: Sexual crimes against women" (2017) 19:3 Crime Prevention and Community Safety 211, online: Springer <https://link.springer.com/article/10.1057/s41300-017-0027-2>

Government Documents

Office of the Information & Privacy Commissioner for British Columbia, *Guidance Document: Using Overt Video Surveillance* (October 2017)

Office of the Information & Privacy Commissioner for British Columbia, *Public Sector Surveillance Guidelines* (January 2014)

APPENDIX A
Survey of Private Establishments and Police Departments

Feedback from private establishments

	CCTV	Retention	Storage	Police Requests	Compliance with PIPA
The Cascade Room [Bar, located in Vancouver]	Surveillance inside the establishment. No street surveillance.	Approx. 48 hours, then recorded over	Onsite drive	Have had police requests in the past. Not aware of any requests for sexual assault investigations.	Not aware of internal policies on the use or storage of CCTV footage.
***Guilt & Co** [Bar, located in Vancouver]	Indoor and street surveillance	Approx. six weeks	Onsite Digital Video Recorder (DVR)	When asked for footage, Guilt & Co. screens footage on-site with PO who has provided case documentation. If "mutually deemed applicable", the footage is downloaded and a copy is made for the PO. Guilt & Co retains a copy and creates "a permanent backup of the entire day's footage." Have received requests for incidents occurring off its premises (street-level footage). Not aware of any footage requests for sexual assault investigations.	No policies on the storage of footage.
Hecklers Bar & Grill [Bar; located in Victoria]	Surveillance inside the establishment. No street surveillance.	Approx. one month	Onsite drive	Have had police requests for theft investigations in the past, but unaware of process for dealing with requests.	Not aware of internal policies on the use or storage of CCTV footage.

Just Dance [Club, located in Vancouver]	No surveillance cameras
Junction [Club; Vancouver]	General Manager stated they were unable to discuss their internal policies.
Colony Bar Main Street [Bar, located in Vancouver]	General Manager stated they were unwilling to participate.

*Guilt & Co. noted that one of their biggest challenges with respect to their surveillance system was “technical”, in that expenditures for maintaining footage of adequate quality was high, and that they faced challenges with balancing the privacy implications of online storage and the “risks” of on-site storage.

Feedback from police departments

We received an email response from the Vancouver Police Department. Their response is as follows:

> "You [sic] question relates to basic search and seizure laws, which all police agencies in Canada must follow. If video evidence of any crime is captured by a private organization, police can typically seize the evidence by consent of the owner or via search warrant. In certain circumstances, police can also seize evidence without warrant (and later obtain a warrant) to prevent destruction of that evidence.
>
> Each investigation is difference [sic], so it is impossible to say how long this process takes. In some cases, video evidence can be retrieved within minutes. In other cases, it could take days or weeks."