Order P21-06

THE OWNERS, STRATA PLAN BCS1964 (ICON 1 AND 2)

Lisa Siew
Adjudicator

June 29, 2021

CanLII Cite: 2021 BCIPC 35
Quicklaw Cite: [2021] B.C.I.P.C.D. No. 35

Summary: A resident of a strata building complained that the strata corporation was in violation of the *Personal Information Protection Act* (PIPA) by inappropriately collecting and using personal information that it obtained through its video surveillance system and its key fob system. The adjudicator concluded the strata corporation was authorized under PIPA to collect and use personal information through its video surveillance system for only some of its specified purposes and for the purposes of creating and updating a key fob inventory. The adjudicator required the strata corporation to stop collecting and using personal information for its other purposes and through its key fob system because those purposes were inappropriate in the circumstances.

Statutes Considered: *Personal Information Protection Act*, ss. 1 (definitions of "contact information", "organization", "personal information", "work product information"), 2, 3(1), 6(2)(a), 7(1), 10(1), 11, 12(1)(h), 14, 15(1)(h), 36(2)(e), 38(2), 47(3)(b), 52(3), 52(4), 53(1); *Strata Property Act*, s. 1(1) (definition of "tenant" and "occupant"), ss. 35, 36, 119 and 130; *Interpretation Act*, s. 1 (definition of "enactment" and "regulation") and s. 29 (definition of "person"); *Limitation Act*, ss. 1 (definition of "claim") and 30 (definition of "pre-existing claim").

INTRODUCTION

[1] A resident of a strata building complained to the Office of the Information and Privacy Commissioner (OIPC) about the strata corporation's use of video surveillance and a key fob system in the strata complex. The complainant alleged the strata corporation, The Owners, Strata Plan BCS1964, (the Organization) was in violation of the *Personal Information Protection Act* (PIPA) by inappropriately collecting, using and disclosing personal information that it obtained through these systems. The complainant also alleged the Organization was not adequately protecting the personal information.

[2] The OIPC investigated the complaint, but the matter was not resolved and it was forwarded to inquiry. The investigation narrowed the issues to the Organization's collection and use of personal information. The complainant no longer disputed the Organization's disclosure and protection of the personal information.

[3] Both parties provided submissions for the inquiry. The OIPC gave the parties an opportunity to revise their submissions to address some information and references about what took place during mediation. To preserve the integrity of the "without prejudice" nature of the mediation process, a party may not, without the written consent of the other parties, refer to or include in its inquiry submissions any information or records related to the mediation process.[1] I also reminded the parties, and provided them with guidance, about the provisions of PIPA relevant to this inquiry as set out in the notice of inquiry.[2]

[4] Before the parties provided their revised submissions, the complainant requested and obtained a general adjournment of the inquiry to pursue a number of complaints against the Organization through the Civil Resolution Tribunal (CRT) process. The CRT has jurisdiction over strata property claims brought under its governing legislation. I understand that process is now complete and a decision was issued in those matters.[3]

[5] After the CRT issued its decision, the complainant requested that the inquiry recommence. After the restart of the inquiry, both parties provided additional submissions.[4] However, some of those submissions still contained references to what occurred at mediation and there was no evidence they had obtained each other's written consent to include this information in their submissions.[5] As a result, the OIPC's registrar of inquiries informed the parties that any references to mediation discussions would not be considered by the adjudicator. Accordingly, I have not taken into account any mediation information or materials in the parties' submissions when making my decision.

---

[1] OIPC's *Instructions for Written Inquiries* at p. 5, dated August 2020.
[2] I also provided the parties with a copy of Order P09-02 and directed them to the OIPC's *Instructions for Written Inquiries*.
[3] A copy of *1893569 Alberta Ltd. v. The Owners, Strata Plan BCS 1964*, 2019 BCCRT 479 was provided in the Organization's submission dated June 9, 2020. This decision is not relevant to the resolution of the PIPA issues before me.
[4] The complainant's submissions are dated September 19, 2018, May 27, 2020 and June 24, 2020. The Organization's submissions are dated August 20, 2018, October 4, 2018, June 9, 2020 and June 30, 2020.
[5] The Organization provided further submissions, but it continued to rely on its initial submissions which contained references to mediation materials and discussions.

PRELIMINARY MATTERS

The conduct of inquiries: review of personal information

[6] The parties accuse each other of breaching PIPA by disclosing the personal information of other individuals in their inquiry submissions. The complainant alleges the Organization "recklessly released the personal information including contact information and signatures of all lot owners without consent when including the list of people who attended an AGM."[6] In response, the Organization accuses the complainant of capturing the personal information of other individuals without consent by providing a photo of a computer screen that allegedly shows "FOB use in real time."[7] This is the full extent of the parties' submissions on this matter.

[7] I conclude it was not a breach of PIPA when the parties in this inquiry provided evidence that contains the personal information of other individuals. Section 17 provides that an organization, which includes a person, may disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.[8] The reasonable person standard is an objective assessment where one has to decide whether the hypothetical reasonable person, knowing the purposes for the disclosure and the surrounding circumstances, would consider those purposes to be appropriate.[9]

[8] In the present case, the parties disclosed the personal information of other individuals for the purpose of providing and exchanging information and evidence to support their position on an issue in this inquiry. There is no evidence that the parties disclosed personal information about another individual for any purpose other than this inquiry. The parties also did not sufficiently explain why it would be inappropriate to provide and exchange the evidence at issue. Based on the materials before me, I find the evidence provided by both parties in this case was appropriate and relevant for the issues to be decided in this inquiry. Therefore, I conclude a reasonable person knowing that the parties' purpose for disclosing the personal information of other individuals was for an OIPC inquiry would consider that purpose appropriate in the circumstances.

[9] Having found the purpose was appropriate, s. 17 also requires that the purpose of the disclosure comply with either ss. 17(a), (b) or (c).[10] Section 17(c) is relevant in this case and it provides that the purposes of the disclosure "are otherwise permitted under this Act." A disclosure of personal information to the Commissioner or their delegate and to an opposing party that is relevant to an

---

[6] Complainant's submission dated September 19, 2018 at p. 4.
[7] Organization's submission dated October 4, 2018 at p. 1.
[8] Order P20-03, 2020 BCIPC 21 (CanLII) at para. 74.
[9] Order P05-01, 2005 CanLII 18156 (BCIPC) at para. 55.
[10] Order P20-03, 2020 BCIPC 21 (CanLII) at para. 74.

inquiry is permitted under ss. 18(1)(o) and 50(1). Section 18(1)(o) allows an organization, which includes a person, to disclose personal information about an individual without their consent if the disclosure is required or authorized by law. The legal authorization for the disclosure that occurred during the conduct of this inquiry is found under s. 50(1) of PIPA.

[10] Section 50(1) empowers the Commissioner or their delegate to conduct an inquiry and decide all questions of fact and law arising in the course of an inquiry. This process necessarily involves the parties providing and exchanging information and evidence to support their position on an issue, which may include the personal information of other individuals as occurred in this case. Under s. 50(1), the Commissioner or their delegate has the authority and discretion to admit, review and assess this information and evidence as part of the OIPC inquiry process to reach a decision on the issues. Further, subject to certain exceptions none of which apply here (e.g. *in camera* material), it is a fundamental principle of procedural fairness that a party has the right to know and respond to the opposing party's case and to know the materials being considered by the adjudicator.

[11] I, therefore, conclude the parties in this inquiry were authorized by law, in this case PIPA, to provide submissions and evidence that discloses personal information about an individual without the consent of that individual for the purposes of an OIPC inquiry. As a result, I find the purpose of the current disclosure complies with s. 17(c) because disclosure without consent is permitted under s. 18(1)(o) of PIPA.

The applicability of the Limitation Act

[12] The Organization submits that one of the matters that the complainant complains about occurred in 2012, so the *Limitation Act* applies and he is barred from raising it.[11] This is the full extent of the Organization's submissions on this matter.

[13] In general, the *Limitation Act* sets out the period of time (referred to as a "limitation period") after which a court proceeding must not be brought with respect to a claim. The *Limitation Act* defines a "claim" as "a claim to remedy an injury, loss or damage that occurred as a result of an act or omission."[12] Given the events associated with the alleged complaint occurred in 2012, the definition of a "pre-existing claim" is also relevant. A "pre-existing claim" is defined as a claim "that is based on an act or omission that took place before [June 1, 2013],"

[11] Organization's submission dated June 9, 2020 at p. 2.
[12] *Limitation Act*, SBC 2012, c. 13 at s. 1. The current *Limitation Act* came into effect June 1, 2013 and replaced the previous Act (*Limitation Act*, RSBC 1996, c. 266).

and "with respect to which no court proceeding has been commenced before [June 1, 2013]."[13]

[14] I am not persuaded that the *Limitation Act* prevents the complainant from submitting a complaint to the OIPC. A complaint made to the Commissioner under PIPA does not qualify as a "claim to remedy an injury, loss or damage that occurred as a result of an act or omission" and the OIPC's complaint process is not a court proceeding. Therefore, I conclude the *Limitation Act* does not apply in these circumstances.

[15] The question remains whether there is a limitation period that applies in these circumstances. Section 47 of PIPA sets out the time period for a complaint to be delivered to the OIPC. Section 47(3)(b) of PIPA allows an individual to make a complaint to the Commissioner at any time.[14] A complaint under s. 36(2)(e) of PIPA includes an allegation that personal information has been collected or used by an organization in contravention of PIPA. As a result, I find the complainant is not time-barred from making this specific complaint to the OIPC for a resolution and I will consider it as part of this inquiry.

ISSUES

[16] The issues that I must decide, as set out in the notice of inquiry, are as follows:

1. Is the Organization's collection and use of personal information through its video surveillance cameras in compliance with s. 6 (consent required), s. 10 (notice for collection), s. 11 (limits on collection) and s. 14 (limits on use) of PIPA.

2. Is the Organization's collection and use of personal information through its key fob system in compliance with s. 6 (consent required), s. 10 (notice for collection), s. 11 (limits on collection) and s. 14 (limits on use) of PIPA.

[17] PIPA does not say who has the burden of proof for an inquiry into the issues identified above. Previous OIPC decisions have found, however, that it will be in each party's interest to provide information and evidence to support and justify their position.[15] I agree with this approach.

---

[13] Subsection 30(1) of *Limitation Act*, SBC 2012, c. 13. Section 30 of the current version of the *Limitation Act* is a transitional provision that addresses claims that existed prior to the effective date of June 1, 2013 and provides that the former version of the *Limitation Act* applies to claims that pre-existed June 1, 2013.
[14] Order P07-01, 2007 CanLII 44884 (BC IPC) at para. 41.
[15] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 4.

[18] In terms of the order in which the issues will be addressed, I will first consider whether the Organization is collecting personal information. If so, I will then address whether the Organization provided notice of its purposes under s. 10 or whether PIPA authorizes the collection without notice. Where notice was provided, I will then consider whether the Organization obtained consent in accordance with s. 6. Lastly, I will consider the appropriateness of the Organization's collection and use under ss. 11 and 14.

DISCUSSION

Background[16]

[19] The Organization is a strata corporation that is responsible for a strata development consisting of 176 strata lots, including townhouses.[17] The strata lots are divided between two complexes located in Vancouver, BC. The first complex is a concrete high-rise building referred to as Icon 1. The complainant is a resident of a strata unit located in Icon 1. The second complex is a lower-rise building referred to as Icon 2. Each Icon building has its own lobby, but both buildings share a number of amenities which are located in Icon 2. These amenities include a concierge service offered 24 hours every day of the week, a fitness room, indoor pool and hot tub.

[20] In 2015, the Organization requested and received approval from the strata unit owners to upgrade the video surveillance system that was originally put in place by the strata developer. The Organization says the original cameras were "outdated, cheap and ineffective"; therefore, it was extremely difficult to identify anyone from the footage.[18] The Organization also explains that part of the upgrade involved adding cameras to the townhouse, patio and courtyard areas because of security issues. The Organization also updated its key fob system in 2015. The Organization says the original key fob system was replaced because it was "falling apart."[19]

[21] In 2016, the Organization adopted a rule about its collection and use of video surveillance footage and key fob information. In 2017, the Organization held an annual general meeting where the strata unit owners voted in favour of adopting this rule as a registered bylaw (Bylaw 44).[20]

[22] There are a number of video cameras in both Icon buildings and the surrounding strata property. The Organization provided a list of the camera

---

[16] The background materials are gathered from the parties' submissions, such as the Organization's submission at Enclosure #1.
[17] The Organization does not identify whether the townhouses are located in both complexes or only one, but nothing turns on this fact.
[18] Organization's submission dated August 20, 2018 at p. 4.
[19] Organization's submission dated June 9, 2020 at p. 1.
[20] Organization's submission dated August 20, 2018 at p. 3 and accompanying documents.

locations.[21] The cameras are located at 18 internal areas, including the lobby, gym, pool, parking areas, elevators and garbage room. There are about 10 external camera locations that include the parkade gate, the courtyard areas, the "Enterphone" entry system and entranceways.

[23] Key fob entry is required for about 30 different locations in the two Icon buildings. The Organization provided a list of those locations, which includes the main lobby and entrance doors, parkade access, elevator access, bike storage, the swimming pool and the fitness room.

Overview of the complaint

[24] The complainant alleges the Organization has been inappropriately collecting and using his and other people's personal information through its video surveillance and key fob system. The complainant says that he is concerned with how the Organization is using this information and who is accessing the information, including how and why this information is collected, stored and disseminated.

[25] I note that the complainant's submissions focus on certain specific locations, but there is no information before me that shows the complainant agreed to narrow his complaints to only certain video cameras and key fob stations.[22] Therefore, I presume that all of the video camera locations and key fob stations are in dispute.

[26] The complainant makes the following allegations and provides the following examples of what he views as the Organization's inappropriate collection and use of personal information:

- The complainant was investigated for a potential rule or bylaw violation regarding a heater installed on the balcony of the strata unit that he occupies. During the investigation, video surveillance footage of the complainant and his guests was allegedly shared with others.

- The complainant claims strata council members and other unnamed individuals were viewing video surveillance footage of individuals in the hot tub. He alleges strata council members at the 2015 annual general meeting were making jokes about watching people in the hot tub area.

- The Organization is routinely monitoring for minor bylaw infractions such as improper garbage disposal and prohibited short-term accommodation. The

[21] The complainant does not dispute where the cameras are located, but accuses the Organization of using additional hidden cameras.
[22] The OIPC investigator's fact report does not identify whether mediation narrowed the dispute to only certain video camera locations or fob stations.

complainant says he was actively monitored in real time and approached and questioned by employees of the Organization to determine if he was violating the Organization's rules and bylaws prohibiting short-term accommodation.

- At the end of August 2018, the Organization released a memorandum informing residents that it was going to use fob and surveillance footage to ensure compliance with a traffic light recently installed in the parkade.

- The strata council has repeatedly expressed its wishes to expand the video surveillance to encompass more minor bylaw enforcement; for example, to catch people discarding cigarette butts in the underground parkade.

- The Organization appears to be collecting personal information from cameras hidden throughout the interior and exterior of the building and it uses personal information for undisclosed reasons.

- The Organization tracks and monitors fob use in real time for bylaw enforcement. The complainant alleges this information was used to deny access to a suite in the building under suspicion of illegally using the suite for short-term accommodation.

- The Organization recently introduced a rule to deny elevator access, and thus unit access, to residents who violate the strata's rules and bylaws. The complainant explains that the rule is implemented by "using the key fob database information to deny access to the elevators by deactivating people's key fob."

[27] The complainant describes the impact of this surveillance as invasive and uncomfortable. He says it forces him to limit access to his strata lot and the common property since someone is always watching him in his home.

Is the Organization collecting personal information?

[28] Section 3(1) states that PIPA applies to every organization. PIPA defines an organization to include "a person, an unincorporated association, a trade union, a trust or a not for profit organization." Under the *Interpretation Act*, a "person" includes a corporation.[23] The Organization is a strata corporation and the parties do not dispute that it qualifies as an organization and is subject to PIPA.

[29] PIPA's stated purpose "is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right

[23] RSBC 1996, c 238 at s. 29.

of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[24] The information that is collected and used by the organization must, therefore, qualify as "personal information" in order for PIPA to apply.

[30] PIPA governs the collection, use and disclosure of "personal information", which it defines as "information about an identifiable individual", including "employee personal information", but excluding "contact information" and "work product information."[25]

[31] The first step in assessing whether information is "personal information" is determining if the information is "about an identifiable individual."[26] In order to qualify as personal information, the information must be reasonably capable of identifying a particular individual either alone or when combined with information from other available sources.[27] Courts have found in various cases that the term "personal information" must be given a broad interpretation to give effect to the legislation's intended purpose.[28]

Video surveillance captures "personal information"

[32] The Organization says its video surveillance system captures picture and video data, but the system does not record audio data.[29] It describes the collected information as a person's image as they enter or leave the area where the cameras are located, including exterior doors and the parking facility. The Organization acknowledges that the cameras capture the complainant's image, along with the images of other owners and occupants.[30]

[33] I conclude the information collected and used by the Organization qualifies as "personal information" under PIPA. The Organization does not dispute that its video surveillance system captures and records "personal information" such as a person's image as they enter, exit and move throughout the building and strata property. The OIPC has also previously determined that video surveillance of an individual amounts to the collection of that individual's personal information and

---

[24] Section 2 of PIPA.
[25] All three terms are defined under s. 1 of PIPA.
[26] Order P13-01, 2013 BCIPC 23 at para. 16.
[27] Order P12-01, 2012 BCIPC 25 at para. 82.
[28] OIPC Investigation Report P18-76168, Joint investigation of The Cadillac Fairview Corporation Limited at para. 61 <https://www.oipc.bc.ca/investigation-reports/3480>, quoting *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 and *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070 para 32.
[29] Letter from Organization's lawyer to complainant, dated January 6, 2017 at p. 1.
[30] *Ibid* at p. 2.

nothing in the evidence here persuades me that a different conclusion should apply.[31]

[34] Video surveillance captures a range of information that may convey detailed information about an individual such as their physical appearance and condition and other aspects of appearance.[32] The video cameras may also record "personal information" in the form of an individual's activities, behaviour, lifestyle, habits, associations with other individuals and patterns of arrival and departure.[33] Further, PIPA does not limit collection to recording alone and collection may occur when the personal information of individuals is collected through live monitoring.[34]

[35] Video recordings of an individual's image qualifies as personal information if the individual is identifiable from the image.[35] However, less visible images of an individual may also qualify as personal information where that individual is directly or indirectly identifiable when combined with other sources of information. For instance, the video footage may not produce recognizable facial images, but other indicators may allow for identification of a person through their clothing, body type, personal effects or objects carried by or associated with a person. Taking all of this into account, I am satisfied that the information captured by the video surveillance system in this case qualifies as personal information.

Key fob system captures "personal information"

[36] The Organization does not dispute that the key fob system collects personal information. It says the key fob system records activity data such as the dates and times a person enters and exits the building and when they access the building's amenities, facilities and elevators.[36]

[37] The Organization does not fully explain how its key fob system works. However, based on the materials before me, I am able to conclude that the system consists of a small-sized key fob, a locking mechanism and a key fob reader affixed near the secured access point or on the door itself. A person may gain access by placing their fob near a reader, or in some cases by pressing a button on the fob, which sends a signal to the reader and releases the locking mechanism.

---

[31] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60 and *Investigation Report P17-01: Use of employee surveillance by a BC chicken catching organization* at p. 8 <https://www.oipc.bc.ca/investigation-reports/2099>
[32] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60.
[33] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60.
[34] Order P19-03, 2019 BCIPC 42 at para. 33.
[35] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60.
[36] Letter from Organization's lawyer to complainant, dated January 6, 2017 at p. 2.

[38] Based on the parties' submissions, I also understand there are two collection points related to the Organization's key fob system:

(1) information collected on a paper form for a key fob inventory, and

(2) information collected electronically by the key fob system.

I will address each of these collection points below.

Key fob inventory

[39] According to the complainant, the Organization updated its fob key system in 2015 so that each fob is now linked to a specific strata lot.[37] As part of the upgrade, the complainant says the Organization recorded the serial number of the fobs and assigned them to a strata lot and a person. The complainant provided evidence which shows that, in 2015, the Organization required residents to fill out a form identifying their unit number, tower number, fob number, name and their status as an owner, agent or tenant of the strata lot.[38]

[40] The Organization does not dispute that owners and residents were required to fill out this form. It says audits are taken from time to time to ensure that it has up to date information on fob allocation, including deactivating key fobs that have been reported as lost, stolen or missing. The Organization refers to this process as a fob audit, but I understand the Organization to mean that it collected information to compile and update a list or inventory of the key fobs held by the strata's owners and residents.

[41] Based on the materials before me, I am satisfied the Organization collected personal information in conducting a key fob inventory. The Organization collected information that identifies a person's name, what strata unit they live in or own, each individual key fob number and the number of key fobs in their possession and whether they are an owner, agent or tenant of the strata unit. I find this collected information is clearly about identifiable individuals.

Key fob system

[42] Based on the parties' submissions, I understand that every time a key fob is used, a key fob reader receives information stored on the key fob. The Organization says "the data on the fob is the unit number of the specific fob and the date and time that it was used for access to a specific area."[39] At this point in time, it is not apparent that the key fob readers are collecting information or that there is an identifiable individual associated with this information. The information

[37] Complainant's submission dated September 19, 2018.
[38] Complainant's submission dated September 19, 2018 and May 27, 2020.
[39] Organization's submission dated August 20, 2018.

received by the reader on its own does not identify who is the registered user of the fob or who is using the fob at that time. It functions as a conventional lock and key system by opening a locked door.

[43] However, from the parties' various submissions, I understand every key fob swipe or use is transmitted back to a computerized database that records each fob use and links that information with other identifying information in the database. The complainant provided a photo of a computer monitor at the concierge desk that he says shows in real time when a key fob is being used, to whom it is registered, and the date, time and location of use.[40]

[44] The Organization does not dispute the complainant's description of what information is stored on the database and that it is viewable on a computer monitor at the concierge desk. Each key fob also has a unique number that is linked to a specific individual. The Organization acknowledges that it keeps a record of who each key fob is assigned to and records the date, time and location of each fob use.

[45] I find the information received by the key fob readers when linked with information in the computerized database qualifies as personal information since it identifies that a key fob registered to a particular strata unit and its owner or occupant was used at a particular date, time and location. For instance, the concierge can determine which specific key fob was used by reviewing the database in real time or by later looking at the recorded information in the database. As a result, the key fob number acts as a conduit to personal information about the registered user that is readily available to the Organization through its databases. The OIPC has previously determined that this type of collection equates to the collection of "personal information".[41]

[46] In addition, the Organization does not dispute that it is collecting personal information with its key fob system. Each key fob is assigned to a specific individual and the parties presume that the registered person is using their assigned key fob. I understand this is what the Organization means when it says the key fob system records a person's location and activity data such as when a person enters and exits the building and when they access the building's amenities, facilities and elevators. Therefore, in those cases, collecting information about a key fob's use also equates to collecting personal information about the registered user's movement into and throughout the strata property.

[47] Further, even when the key fob is not being used by the fob's registered user, the collected information is reasonably capable of identifying a particular

---

[40] Complainant's submission dated September 19, 2018.
[41] Order P12-01, 2012 BCIPC 25 (CanLII) at paras. 98-113 and Investigation Report F12-04, 2012 BCIPC No. 23 <http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-04.pdf>.

individual's movements when combined with other available information. It would clearly be a simple matter for the Organization to use video surveillance footage, the concierge's observations or eyewitness accounts to determine the identity of the person using a key fob at a specific location, date and time. Therefore, for all these reasons, I conclude that collecting information about a key fob's use is a collection of personal information regarding identifiable individuals and their activities.

Is the information contact or work product information?

[48] The second step is to determine whether the information collected and used by the Organization is excluded from the definition of "personal information" because it is "contact information" or "work product information."[42] I conclude the collected information does not qualify as "contact information" or "work product information" as those terms are defined under s. 1 of PIPA and interpreted by previous OIPC orders.[43] I, therefore, conclude the information collected from the video surveillance system, for a key fob inventory and from the key fob system qualifies as personal information.[44]

Is notification required for the collection?

[49] Having found the Organization is collecting personal information, the next step is to determine whether the Organization provided notification of its purposes in accordance with s. 10(1) or whether PIPA authorizes the collection without notice. For instance, under s. 10(3), the required notification under s. 10(1) does not apply to a collection described in ss. 8(1) and 8(2) where consent is deemed to be given. Section 8(1) does not require notice because an organization's collection purpose would be obvious to a reasonable person.

[50] As well, there are provisions under s. 12(1) where PIPA authorizes the collection without consent and by implication without notice. For example, s. 12(1)(b) allows an organization to collect personal information about an individual without consent or from a source other than the individual where the collection is necessary for the medical treatment of the individual and the individual is unable to give consent. Under those circumstances, direct notification to the individual may not possible, but PIPA authorizes the collection.

---

[42] Order P13-01, 2013 BCIPC 23 at para. 16.
[43] Order P12-01, 2012 BCIPC 25 (CanLII) at para. 96 and Order P14-03, 2014 BCIPC 49 (CanLII) at para. 19 for an interpretation of "work product information."
[44] I have also considered the fact that the video surveillance system and the key fob system captures the personal information of the Organization's employees (e.g. the concierge and a strata council member). However, none of the employees submitted a complaint to the OIPC about the Organization's collection and use of their personal information. I have, therefore, only focused on the complainant's concerns as a resident of the strata building.

[51] In terms of the groups of individuals that the Organization needs to notify of its collection purposes, I note that the *Strata Property Act* identifies "three classes of persons who will inhabit and interact with a strata corporation: owners, tenants and occupants."[45] A tenant is defined in s. 1(1) of the *Strata Property Act* as a person who rents all or part of a strata lot and includes a subtenant. An "occupant" is defined as a person, other than an owner or tenant, who occupies a strata lot. I may, at times throughout this order, collectively refer to tenants and occupants as residents. I also find any visitors to the strata complex such as guests of owners or residents, couriers, delivery drivers or tradespeople will be affected by the Organization's collection of personal information.

[52] The Organization submits that it has fulfilled the notice requirements under s. 10; therefore, I will first consider whether the Organization's collection and use fulfills the purposes that it discloses under s. 10(1). If not, I will then consider whether PIPA authorizes the collection without notice.

Did the Organization provide notice in accordance with s. 10(1)?

[53] Section 10(1)(a) says that on or before collecting personal information about an individual from the individual, the organization must disclose to the individual, either verbally or in writing, the purposes for the collection of the information. The first step in the s. 10(1) analysis is to identify an organization's purpose for collecting the personal information. This purpose should be stated as precisely as possible so that the needs of the organization to collect and use the information can be carefully assessed against the privacy rights of the individual.[46]

[54] In this case, the Organization says its purpose for collecting and using the personal information at issue is for security and safety reasons. The Organization submits that its security measures have been taken to protect the strata property from theft and damage and to protect the health and welfare of the owners.

[55] To be more precise, the Organization submits that the video camera footage is needed for the following purposes:

- To prevent, detect and investigate break-ins and thefts.
- To prevent and investigate any damage to strata property.
- To ensure the safety of owners, residents and visitors and provide emergency aid.

[45] *Kunzler v. The Owners, Strata Plan EPS 1433*, 2020 BCSC 576 (CanLII) at para. 49.
[46] Order P11-02, 2011 BCIPC 16 at para. 71.

- For bylaw enforcement such as investigating complaints, ensuring proper garbage disposal and preventing inappropriate behaviour on common property.

[56] The Organization submits that the key fob information is needed for the following specific purposes:

- To monitor access to the strata complex for security and safety reasons.

- To create and maintain a key fob inventory to manage lost or stolen fobs.

[57] The second step is to consider whether the Organization disclosed its purposes verbally or in writing to the individual on or before collecting personal information from that individual. The notice required under s. 10(1)(a) must be detailed enough to identify the particular purpose for collecting the information, as distinct from other purposes, in a way that is understandable to a member of the public.[47]

[58] The Organization submits that Bylaw 44 is a "complete answer" to the notice provisions under s. 10.[48] It reads:

> 44. Video Usage in Common Areas
>
> (1) Closed circuit television and video surveillance are installed in many common areas of the Icon complex. The system operates 24 hours a day and the Strata Corporation collects data from the closed circuit television and video usage.
>
> (2) The Strata Corporation collects data with respect to the usage of each security fob programmed for use at Strata Plan BCS1964.
>
> (3) The video files and/or security fob usage records will be used by the Strata Corporation for surveillance and monitoring purposes only, including the following purposes:
>
> a) being alerted to the presence of trespassers on the strata plan;
>
> b) preventing, recording, investigating and obtaining evidence of any theft, vandalism, nuisance or damage caused by any person on the strata plan;
>
> c) ensuring the safety of the complex owners, tenants, occupants and visitors; and

[47] Order P11-02, 2011 BCIPC 16 at para. 104.
[48] Cover letter to Organization's submission dated August 20, 2018.

> d) enforcing those Strata Corporation bylaws and rules which relate to theft, vandalism, nuisance or damage caused by any person on the Strata Plan; the safety and security of the strata plan and the complex owners, tenants, occupants and visitors.[49]

[59] For the reasons to follow, I am satisfied that someone reading Bylaw 44 would only understand some of the purposes for which the Organization is collecting personal information. I will consider the Organization's specified purposes below.

To prevent, detect and investigate break-ins, thefts and property damage

[60] Bylaw 44 states the video files will be used by the Strata Corporation for surveillance and monitoring purposes only, including preventing, recording, investigating and obtaining evidence of any theft, vandalism, nuisance or damage caused by any person on the strata plan. I find this wording is sufficient notice that the Organization is collecting personal information from its video surveillance system for two of its purposes: (1) to prevent, detect and investigate break-ins and thefts, and (2) to prevent and investigate property damage.

[61] I am also satisfied the Organization provided owners with a copy of Bylaw 44. The Organization provided part of the meeting minutes from its February 27, 2017 annual general meeting which says, "The below proposed Bylaw was adopted by the Strata Council as a Rule during a Strata Council Meeting, held on December 12th 2016."[50] The meeting minutes also show that Bylaw 44 was approved at this meeting by a majority of its owners. Therefore, I find that owners were given notice of these two specified purposes by February 2017, if not earlier, considering the proposed bylaw was adopted as a strata rule in 2016.

[62] I find it reasonable to conclude that any new owners or tenants since the February 2017 annual general meeting would also have read or been given access to the Organization's bylaws, so received notice of these two purposes. Strata corporations are required to have bylaws and must make them available upon request to strata owners or their assignees.[51] Further, none of the parties said so, but I am aware that a strata corporation's bylaws are a necessary part of the disclosure requirements for any real estate transaction or tenancy agreement.[52]

[63] I note, however, that s. 10(1) of PIPA requires that on or before an organization collects personal information about an individual from the individual, the organization must give that individual, which includes visitors to the strata

---

[49] A copy of Bylaw 44 was provided in the Organization's submission dated August 20, 2018.
[50] Organization's submission dated August 20, 2018 at p. 4.
[51] *Strata Property Act*, SBC 1998, c 43 at ss. 35, 36 and 119.
[52] For instance, as part of issuing "Form K: Notice of Tenant's Responsibilities," a landlord must provide a tenant with a copy of the strata's bylaws.

complex, the appropriate notification.[53] The Organization does not describe what notice is given to visitors, who typically will not have read or heard about Bylaw 44. However, it provided a photo of a sign posted at one of the exterior doors that features a picture of a video camera and reads:

> This Building is Under 24 Hour
> Surveillance for Security Purposes
> For Info Please Call [phone number].[54]

[64] I am satisfied that the wording of this sign, along with the picture of the video camera, sufficiently notifies visitors using this particular door that the purpose of the 24-hour video surveillance is to prevent and identify individuals who commit break-ins or thefts and who intentionally or unintentionally damage strata property. I conclude the term "security purposes" is commonly associated with the security of property and people, which includes preventing and investigating unauthorized entry, theft or property damage. I can also see from the photo that the sign is posted on an exterior door and it is clearly visible.

[65] I note there is clearly more than one entrance to the strata complex; therefore, there should be appropriate signage at those entrances and for any area under video surveillance. The Organization says in its submissions there are signs stating "the video is for security purposes" posted in every area of the property where there are cameras.[55] I accept the Organization's submission that there are similar signs to the one noted-above prominently displayed to visitors before they enter an area under video surveillance. The applicant does not dispute what the Organization says about the content of those other signs and their locations.

[66] To summarize, by providing a copy of Bylaw 44, I find the Organization has notified strata owners and residents that it is collecting personal information from its video surveillance system to prevent, detect and investigate break-ins, thefts and to prevent and investigate property damage. I also accept the Organization provided sufficient notice to visitors of those purposes under s. 10(1) by posting appropriate signage in every area of the strata property where there are video cameras.

For bylaw enforcement

[67] I also find Bylaw 44 provides sufficient notification that the Organization is using video surveillance to enforce bylaws and rules related to "theft, vandalism, nuisance or damage" and the safety and security of the strata complex and of the owners, residents and visitors. However, I am not satisfied that Bylaw 44 on its

[53] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 52.
[54] Organization's submission dated June 9, 2020.
[55] Organization's submission August 20, 2018 at p. 1.

own without posted signs sufficiently notifies individuals that the Organization is collecting personal information from the video surveillance system to enforce its garbage disposal bylaws. The notice required under s. 10(1)(a) must be detailed enough to identify the particular purpose for collecting the information, as distinct from other purposes, in a way that is understandable to a member of the public.[56]

[68] Bylaw 44 states the video files will be used by the Strata Corporation for surveillance and monitoring purposes only, including enforcing those Strata Corporation bylaws and rules which relate to "nuisance" caused by any person on the Strata Plan. I find the Organization's use of the term "nuisance" in Bylaw 44 too imprecise and not detailed enough to distinguish this particular purpose from other activities that may qualify as a "nuisance" such as noises, smells or other disturbances that may affect a person's use and enjoyment of property.

[69] In terms of signage, I note that the Organization says there is signage in the garbage rooms. It says "these rooms did and do have signs indicating area is monitored."[57] However, it did not provide me with a copy of those signs or identify what they say.

[70] The complainant did, however, provide a photo of a sign posted outside the entrance to the garbage and recycling room which reads:

NO HOUSEHOLD ITEMS OF
ANY KIND TO BE LEFT IN THE
GARBAGE ROOM.

AN IMMEDIATE $200 FINE AND
A $150 PER ITEM DISPOSAL
FEE WILL BE ASSESSED FOR
ANY ITEMS LEFT IN THIS GARBAGE ROOM.

24 HR VIDEO MONITORING IN EFFECT.[58]

[71] I find this sign posted by the entrance to the garbage and recycling room informs owners, residents and visitors that 24 hour video surveillance is being used to prevent the improper dumping of garbage. From the photo, I can see that the sign is prominently displayed by the entrance and it is clearly visible. Although the sign does not directly convey there is a bylaw about proper garbage disposal, I conclude this sign qualifies as sufficient notice, under s. 10(1), to owners, residents and visitors that the Organization is using video surveillance to

[56] Order P11-02, 2011 BCIPC 16 at para. 104.
[57] Organization's submission dated August 20, 2018 at p. 3.
[58] The photo was included in the Complainant's submission dated September 19, 2018. The complainant also provided a picture of a sign posted inside the garbage and recycling room; however, the wording on the sign was not clear or legible in the photo.

enforce the substance of the Organization's garbage disposal bylaws, specifically to prevent the improper dumping of garbage.

To ensure safety and provide emergency aid

[72] Bylaw 44 says the video files will be used by the Organization for surveillance and monitoring purposes only, including "ensuring the safety of the complex owners, tenants, occupants and visitors." The Organization explains that the video cameras allow the concierge to monitor multiple areas and to provide owners, residents and visitors with aid when necessary, specifically emergency aid such as heart attacks and drownings in the pool and gym area. However, I am not satisfied that someone reading Bylaw 44 would understand the Organization is collecting personal information from its video surveillance system to provide emergency aid to owners, residents and visitors.

[73] The notice under s. 10(1) should be clear enough that a reasonable person would understand that the information is being collected to provide assistance during health emergencies and for lifeguarding purposes. I do not think that someone reading the phrase "ensuring the safety of the complex, owners, tenants, occupants and visitors" would understand that this wording includes health or life-saving emergencies for the entire strata complex. There was no evidence that strata corporations normally take on this type of liability. In my view, the term "safety" is too broad to encompass providing assistance during health or life-threatening emergencies.

[74] I note the complainant provided a photo of a sign posted in the swimming pool area that has a picture of a video camera and reads:

> This Building is Under 24 Hour
> Surveillance for Security Purposes
> And Bylaw Enforcement[59]

[75] The Organization says the "sign was removed a number of years ago and there is currently no sign to this effect on the pool or gym door."[60] It says there are new signs on the exterior of the building, but as previously discussed, the only photo provided was of a sign posted on one exterior door that says "This Building is Under 24 Hour Surveillance for Security Purposes." The Organization also says there are signs stating "the video is for security purposes" posted in every area of the property where there are cameras.[61]

[76] I accept that the term "security purposes" can include security of people to ensure their safety and to protect against threats or assaults. However, I am not

[59] Photo included in complainant's submissions dated May 27, 2020.
[60] Organization's submission dated June 9, 2020 at p. 2.
[61] Organization's submission August 20, 2018 at p. 1.

satisfied that the wording on these signs provide sufficient notice to owners, residents and visitors that the Organization is recording and monitoring their image and actions to provide assistance during health emergencies or for lifeguarding purposes in the swimming pool area. I conclude that someone reading such signs would not meaningfully understand that the Organization is collecting personal information for those purposes.

[77] Since the Organization did not provide sufficient notice of this purpose, I have considered whether there are any circumstances under s. 12(1) that allows the Organization to collect the personal information without notification. Section 12(1)(h) is the only provision at issue because of the Organization's submission that Bylaw 44 is a complete answer to its collection of personal information. Section 12(1)(h) authorizes an organization to collect personal information about an individual without consent where the collection is required or authorized by law.

[78] Section 119 of the *Strata Property Act* allows strata corporations to pass bylaws that "provide for the control, management, maintenance, use and enjoyment of the strata lots, common property and common assets of the strata corporation and for the administration of the strata corporation."[62] For reasons I will discuss further in this order under the provisions regarding consent, I accept that s. 12(1)(h) may include a bylaw that authorizes a strata corporation to collect and use personal information for appropriate purposes.

[79] However, for the reasons previously given, I conclude Bylaw 44 does not sufficiently identify that the strata corporation is collecting and using personal information to provide emergency aid to owners, residents and visitors. As a result, I find there is no bylaw authorizing the Organization to collect and use personal information for such a purpose.

[80] Furthermore**,** the fact that a strata corporation may have such a bylaw does not dispense with the need for notification. A part of PIPA's purpose is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes the right of individuals to protect their personal information. However, an individual cannot protect their personal information and exercise their rights under PIPA if they do not know an organization is collecting that information. For instance, without notification, individuals would be unable to utilize provisions under PIPA that hold organization's accountable for how they use and secure that personal information or request access to their personal information from an organization.

[81] I also note that a strata corporation is normally required to notify and obtain the majority consent of the strata unit owners in order to obtain approval for a bylaw; therefore, notification is an integral part of the bylaw approval

[62] *Strata Property Act*, SBC 1998 c. 43 at ss. 119 and 120.

process. In order for someone to approve or to follow a bylaw, they have to know about it. Furthermore, this is not a situation where the Organization is unable to provide direct notification to an individual on or before collecting their personal information such as in the case of ss. 12(1)(b) or that notification would compromise the purpose of the collection such as with ss. 12(1)(c). Instead, it would be a simple matter for the strata corporation to post appropriate signage about its collection purposes. As a result, I conclude the Organization would still have notification responsibilities even though an appropriate bylaw and s. 12(1)(h) may allow it to collect personal information without consent.

To monitor access to the strata complex by owners and residents

[82] Bylaw 44 says the Organization "collects data with respect to the usage of each security fob programmed for use at Strata Plan BCS1964" and that it does so for "surveillance and monitoring purposes only", which includes the purposes listed under paragraph 44(3)(a) to (d) of Bylaw 44 that consists of security and safety reasons. The Organization says the personal information collected from the key fob system is needed "to monitor access to the building by bona fide owners and residents, including elevators, which provides a significant level of security for owners and residents."[63]

[83] I find the wording of Bylaw 44 is sufficient notice that the Organization is collecting information about the key fob usage of any owners or residents for the purposes of monitoring access to the strata complex and for security and safety reasons. As for visitors, there was no evidence that visitors are issued key fobs and that the Organization is collecting any of their personal information to monitor and track their key fob usage. Therefore, I conclude the Organization is not required to notify visitors of the reasons why it is collecting personal information from the key fob system.

To create and update a key fob inventory

[84] Bylaw 44 does not say that the Organization is collecting personal information for the purposes of a key fob inventory and what that entails. In my view, the wording of Bylaw 44 is not sufficient to allow an individual to understand that the Organization is collecting personal information for this particular purpose. I, therefore, conclude that Bylaw 44 does not fulfill the notice requirements under s. 10(1) of PIPA.

[85] I have also considered whether the form that owners and residents are required to complete provides the required notice. The form is titled "2015 Fob Audit" and there is a space for owners and residents to write their unit number, fob number and name. Owners and residents are also informed of the following:

[63] Letter to complainant from Organization's legal counsel dated March 9, 2017 at p. 3.

> The fob number is the five digit PIN number on the back of the fob. If you cannot read it, please contact the Concierge Desk for assistance. Fobs marked as unreadable will be deactivated.[64]

[86] On its own, the form is not sufficient notice. However, after the security upgrades, the strata council told owners and residents that it needed to conduct an audit of the key fobs for security reasons.[65] As a result, I understand that there was further information provided by the strata council to owners and residents about why the Organization was collecting the personal information and what it would be used for. Considering all this information, I conclude the Organization notified owners and residents that it was collecting personal information for the purpose of creating and maintaining a key fob inventory.

[87] As for visitors, there was no evidence that visitors are assigned key fobs and that the Organization is collecting any of their personal information to create and maintain a key fob inventory. Therefore, I conclude the Organization is not required to notify visitors of this particular purpose.

Summary regarding notification

[88] By providing a copy of Bylaw 44, I find the Organization has notified owners and residents that it is collecting personal information from its video surveillance system or key fob system for the following purposes:

- To prevent, detect and investigate break-ins and thefts.
- To prevent and investigate damage to strata property.
- To enforce bylaws and rules related to theft, vandalism, nuisance or damage and the safety and security of the strata complex, the owners, residents and visitors.
- To ensure the safety of the complex owners, tenants, occupants and visitors against threats or assaults.
- To monitor access to the strata complex for security and safety reasons by collecting information about the key fob usage of any owners or residents.

[89] I also conclude the Organization notified owners and residents that it was collecting personal information for the purpose of creating and maintaining a key fob inventory.

---

[64] A copy of this fob audit form is located in the Complainant's submission dated May 27, 2020.
[65] Complainant's submission dated September 19, 2018 at p. 2.

[90] As well, by posting appropriate signage, I find the Organization has notified owners, residents and visitors that it is collecting personal information from the video surveillance system to enforce its garbage disposal bylaws. I also accept there is appropriate signage that notifies visitors that the Organization is collecting and using personal information from its video surveillance system to prevent and investigate break-ins, thefts and property damage and to ensure the safety of owners, residents and visitors against threats or assaults.

[91] However, I conclude the Organization has not provided sufficient notice to owners, residents and visitors that the Organization is recording and monitoring their image and actions to provide assistance during health emergencies that may occur throughout the strata complex and for lifeguarding purposes in the swimming pool area.

Was there consent for the collection and use?

[92] My analysis and conclusions in this section will consider both collection and use since the requirements around consent apply equally to both. Section 6 of PIPA requires organizations to obtain an individual's consent before collecting and using their personal information. PIPA also provides limited circumstances that allow an organization to collect and use personal information where the individual is deemed to have consented (s. 8) or PIPA authorizes the collection and use without consent (ss. 12 and 15).

Collection and use without consent – ss. 12(1)(h) and 15(1)(h)

[93] The Organization submits that Bylaw 44 is a "complete answer" to the consent provisions of PIPA.[66] Sections 12(1)(h) and 15(1)(h) of PIPA are relevant in this case. Even though the notice of inquiry and the parties did not directly refer to these provisions, they are part of the consent provisions under s. 6 and I will consider them since they apply to the circumstances here and the parties had an opportunity to make submissions about these provisions.[67]

[94] Sections 12(1)(h) and 15(1)(h) stipulate that an organization may collect or use personal information about an individual without consent if the collection or use is required or authorized by law. PIPA does not define the term "law"; however, previous OIPC orders have relied on the definition of an "enactment" under the *Interpretation Act* to determine whether something qualifies as a law under PIPA.[68] I adopt that approach to determine whether Bylaw 44 qualifies as a law under PIPA.

---

[66] Cover letter attached to Organization's submission dated August 20, 2018.
[67] I referred to ss. 12(1) and 15(1) in my letter to the parties dated December 5, 2018.
[68] Order P20-03, 2020 BCIPC 21 (CanLII) at paras. 67-68 and Order P06-01, 2006 CanLII 13537 at para. 44.

[95] Section 1 of the *Interpretation Act* states that an "enactment" includes a "regulation" which is then defined to include "a bylaw…enacted…in execution of a power conferred under an Act." I conclude s. 119 of the *Strata Property Act* confers upon strata corporations the power to pass bylaws that authorize the collection and use of personal information for appropriate purposes. Therefore, I am satisfied that a strata corporation's bylaws are an "enactment" and thus a "law" for PIPA's purposes.

[96] As a result, I find that Bylaw 44 authorizes the Organization to collect and use personal information without consent for the specific purposes that I found are covered under the language of Bylaw 44. To be clear, those purposes are as follows:

- To prevent, detect and investigate break-ins and thefts.
- To prevent and investigate damage to strata property.
- To enforce bylaws and rules related to theft, vandalism, nuisance or damage and the safety and security of the strata complex, the owners, residents and visitors.
- To ensure the safety of the complex owners, tenants, occupants and visitors against threats or assaults.
- To monitor access to the strata complex for security and safety reasons.

[97] I find this authorization to collect and use personal information without consent for the above-noted purposes applies not only to the personal information of owners and residents, but also to the personal information of individuals who visit the strata complex. Under the *Strata Property Act*, the legislature has given strata owners the collective right to govern their community and pass bylaws that control and manage the use and enjoyment of strata lots, common property and common assets.[69] A visitor to that strata community would be subject, where relevant, to the bylaws of the strata corporation.[70]

[98] The strata owners, in this case, acting collectively voted to adopt Bylaw 44 and use electronic surveillance for certain purposes throughout the strata complex. Bylaw 44 expressly contemplates that the personal information of visitors would be captured by the Organization's electronic surveillance in order

[69] This authority is subject to certain limitations such as s. 121(1)(a) of the *Strata Property Act* which prohibits a bylaw that contravenes the *Human Rights Code*.
[70] For instance, s. 3 of the Schedule of Standard Bylaws in the *Strata Property Act* requires a visitor not to cause a nuisance or to damage common property or common assets. The Schedule of Standard Bylaws applies to every strata corporation, unless a strata corporation files different bylaws in the land title office.

to achieve its purposes. Therefore, I am satisfied that Bylaw 44 is intended to apply to the personal information of owners, residents and visitors. For instance, one of the purposes identified in Bylaw 44 is to ensure not only the safety of the strata unit owners, tenants and occupants, but also that of visitors. Bylaw 44 also averts the need for the Organization to establish that it obtained an individual's consent every time its electronic surveillance system collects their personal information.[71]

Consent from the individual or deemed consent – ss. 6(2), 7(1) and 8

[99] I found that Bylaw 44 does not provide sufficient notice of the Organization's collection and use of personal information for the purposes of enforcing its garbage disposal bylaws, to create and maintain a key fob inventory and to provide assistance during health emergencies. Therefore, for those purposes, the Organization is either required to obtain consent directly from the individual in accordance with ss. 6(2)(a) and 7(1) or s. 8 must apply where the individual is deemed to have consented to the collection and use.

[100] Section 6(2)(a) provides that an organization must not collect or use personal information about an individual unless the individual consents to the collection or use. Section 7 specifies what constitutes consent for the purposes of PIPA.

[101] First, under s. 7(1)(a), the organization must have provided the individual with the information required under the notice provisions in s. 10(1). This ensures that the individual whose personal information will be collected is aware of the purposes for collecting that information.[72] Notice must be given of the particular purpose with sufficient detail that allows the individual to consent meaningfully and make an informed decision.[73]

[102] Second, under s. 7(1)(b), the individual's consent to the collection and use must have been provided in accordance with PIPA. Where s. 6(2)(a) applies, the individual's consent will be in accordance with PIPA where there is evidence the individual consented to the Organization's collection and use of their personal information.

[103] I will consider each of the three purposes below and first consider whether the Organization obtained consent directly from the individual in accordance with ss. 6(2)(a) and 7(1). If those requirements are not satisfied, I will then consider the provisions under s. 8 regarding deemed consent.

---

[71] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 56.
[72] *Investigation Report P17-01: Use of employee surveillance by a BC chicken catching organization* at p. 11 <https://www.oipc.bc.ca/investigation-reports/2099>.
[73] Order P11-02, 2011 BCIPC 16 at paras. 104 and 106.

To enforce garbage disposal bylaws

[104] I previously found the Organization provided notice in accordance with s. 10(1) by posting a sign by the entrance to the garbage and recycling room that informs owners, residents and visitors that 24-hour video surveillance is being used to prevent improper dumping of garbage. Therefore, I find the Organization has complied with s. 7(1)(a).

[105] Furthermore, I conclude that an individual who reads the sign and decides to enter the garbage and recycling room has consented to the collection and use of their personal information in accordance with s. 6(2)(a). The sign is appropriately placed before an individual enters the garbage and recycling room which affords the individual an opportunity to not enter the area under surveillance if they do not wish to have their image recorded or activities monitored. As a result, I find the consent requirements under ss. 6(2)(a) and 7(1) are satisfied for this specific purpose.

To create and update a key fob inventory

[106] I previously found notice was given in accordance with s. 10(1) because the Organization informed owners and residents of the reason why it was collecting their personal information by providing the "2015 Fob Audit" form and through additional information provided by the strata council. Therefore, I find that s. 7(1)(a) is met for this purpose.

[107] As for evidence of consent under s. 7(1)(b), the complainant says that he did not consent to the Organization collecting and using his personal information through the key fob system.[74] I understand the complainant to mean that he objects to the Organization collecting and using his personal information to track his movements into and throughout the strata property.

[108] The complainant does not discuss consent regarding a key fob inventory, but his submissions indicate that he did participate and complete the relevant form. I note the following passage from the complainant's submission:

> After the security upgrades, Strata Council and their Agents said that they needed to have an audit of these key fobs for security reasons. Again I, and as I am sure, most other lot owners took the organizations request as being in earnest. During this process they recorded the serial number of the fobs and assigned them to the strata lot and person it was registered to.[75]

[74] Complainant's submission dated June 24, 2020 at p. 1.
[75] Complainant's submission dated September 19, 2018.

[109] Therefore, based on the materials before me, I am satisfied that the complainant completed and submitted the "2015 Fob Audit" form to the Organization and understood the reason for the collection and use of his personal information in providing the form. As a result, I find the complainant consented to the Organization's collection and use of his personal information for the purpose of creating and updating a fob inventory. I am, therefore, satisfied that consent was provided in accordance with ss. 6(2)(a) and 7(1)(b) for this particular purpose.

To provide assistance during health emergencies

[110] I previously found the Organization failed to provide sufficient notice to owners, residents and visitors that it is recording and monitoring their image and actions to provide assistance during health emergencies that may occur throughout the strata complex, including the gym and swimming pool area. Therefore, I conclude the Organization did not satisfy the notification requirements under s. 7(1)(a) and failed to obtain consent directly from individuals in accordance with s. 6(2)(a).

[111] Turning to ss. 8(1) and 8(2), I find that none of the circumstances where consent is deemed to be given apply in this case. Section 8(2) applies where the personal information is collected for enrolment or coverage under an insurance, pension, benefit or similar plan, policy or contract, which I conclude does not apply to the facts and circumstances here.

[112] Under s. 8(1), deemed consent exists where, at the time the deemed consent is given, the purpose of collecting the information would be obvious to a reasonable person and the person voluntarily provides the information to the organization for that purpose. Section 8(1) does not require notice because an organization's collection purpose would be obvious to a reasonable person. I do not find that to be the case here.

[113] There was no evidence that strata corporations normally take on this type of liability so that this particular purpose would be obvious to someone who sees the video cameras located in various spots throughout the strata property. Even in the gym and swimming pool area, I find a reasonable person would not expect a strata corporation to be watching them through the video cameras to provide emergency assistance as they workout, swim in the pool or relax in the hot tub. Instead, I conclude a reasonable person would expect these private recreational facilities to operate on a "use at your own risk" policy.

[114] Therefore, for all these reasons, I am not satisfied that a reasonable person who moves throughout the strata complex would consider it obvious that the Organization is recording and monitoring their image and actions in order to provide assistance during a health emergency. As a result, I find this is not a

case of deemed consent under s. 8(1) since the Organization's particular purpose, at the time consent is deemed to be given, would not be obvious to a reasonable person.

Summary regarding consent

[115] With one exception, I find the Organization was authorized under PIPA to collect and use personal information without consent or that it obtained consent in accordance with PIPA. The only exception is the Organization's collection and use of personal information to provide assistance during health emergencies. I conclude the Organization was required to obtain consent directly from the affected individuals in accordance with s. 6(2)(a) for this particular purpose, but it did not satisfy the notification requirements under s. 7(1)(a).

Would a reasonable person consider the Organization's collection and use of personal information to be appropriate?

[116] Having addressed notification and consent, I will now consider whether the Organization's specified purposes are appropriate under ss. 11 and 14. Sections 11 and 14 stipulate that an organization may collect and use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that fulfill the purposes that the organization discloses under s. 10(1), or as otherwise permitted by PIPA.

[117] I have chosen to consider ss. 11 and 14 at the same time since the language used in the provisions governing collection under s. 11 and the use of personal information under s. 14 are almost identical, which means the reasonable person standard applies to the analysis under both ss. 11 and 14.[76] Further, for the most part, the parties' submissions show that the Organization's purposes for collecting personal information are the same as its purposes for using that personal information. Therefore, my analysis and conclusions would apply to both ss. 11 and 14.

[118] Sections 11 and 14 create an "overarching requirement" that the purposes for the collection and use of personal information be appropriate.[77] Even where a person consents, PIPA prohibits the collection of their personal information unless, assessed against an objective standard and in context, the purposes for which it is collected and used are appropriate.[78] Put another way, if an

[76] Order P09-02, 2009 CanLII 67292 (BC IPC) at paras. 54-55.
[77] Order P11-02, 2011 BCIPC 16 (CanLII) at para. 65, overturned for other reasons at *Economical Mutual Insurance Company v. British Columbia (Information and Privacy Commissioner)*, 2013 BCSC 903 (CanLII).
[78] Order P11-02, 2011 BCIPC 16 (CanLII) at para. 67.

organization's purpose is inappropriate in the circumstances, then it "cannot be rendered appropriate via consent."[79]

[119] Based on my review of past authorities, I conclude the analysis under ss. 11 and 14 consists of the following steps:[80]

1. Is the organization's purpose for collecting and using personal information one that a reasonable person would consider appropriate in the circumstances?

2. If the purpose is appropriate, then does the purpose of the collection and use fulfill the purposes that the organization discloses under s. 10(1) or is it otherwise permitted under PIPA?

[120] I will consider each stage of the analysis below, but only where necessary. For instance, if I find a reasonable person would consider the Organization's purposes to be inappropriate in the circumstances, then the Organization's collection and use of the personal information would be in contravention of PIPA. As a result, it would not be necessary for me to move on to the next step and also consider if the purpose for collecting and using the information fulfills the purpose that the Organization discloses under s. 10(1) or is otherwise permitted under PIPA.

1) Are the purposes for the collection and use appropriate?

[121] The first step in the s. 11 and s. 14 analysis is to consider whether the Organization's purposes are "appropriate in the circumstances" in the eyes of a reasonable person. PIPA prohibits the collection and use of an individual's personal information unless the purposes for the collection and use are appropriate when assessed against an objective standard and taking into account relevant circumstances. This standard is described as the "reasonable person" standard where one has to decide whether the hypothetical reasonable person, knowing the purposes for the collection and use and the surrounding circumstances, would consider those purposes to be appropriate.[81]

---

[79] OIPC Investigation Report P20-81997, Joint investigation of Clearview AI, Inc. at p. 4 <https://www.oipc.bc.ca/investigation-reports/3505>. For a similar conclusion, see Order P2006-011, 2008 CanLII 88763 (AB OIPC) at para. 52 where Alberta's former Commissioner Work stated, "…a Complainant cannot consent to the unreasonable collection of personal information under the Act or, in other words, an unreasonable collection cannot be ratified by consent."
[80] For example, Order P11-02, 2011 BCIPC 16 (CanLII), overturned for other reasons at *Economical Mutual Insurance Company v. British Columbia (Information and Privacy Commissioner)*, 2013 BCSC 903 (CanLII).
[81] Order P05-01, 2005 CanLII 18156 (BCIPC) at para. 55.

[122] Previous orders have considered some of the following factors in applying the reasonable person standard:[82]

- Does a legitimate issue exist to be addressed through the collection and use of personal information?
- Has the organization tried or considered other reasonable, less intrusive alternatives to fulfill its purposes?
- Is there a reasonable likelihood that the collection of the personal information will be effective in addressing the legitimate issue?
- Is the collection of personal information carried out in a reasonable manner?
- The kind, nature and sensitivity of the information.
- The uses to which the information will be put and any disclosures the organization intends at the time of collection.
- How long the personal information will be retained.
- Whether the organization is collecting or using the minimum amount of information reasonably required to achieve its purposes.

[123] This list is not exhaustive since other factors may apply depending on the particular circumstances and which factors are relevant will vary from case to case.

[124] I will first consider whether the purposes for the Organization's collection of personal information through its video surveillance system are appropriate and then consider the appropriateness of the Organization's purposes for collecting personal information through its key fob system.

[125] Before doing so, a circumstance that I find relevant to all of the Organization's purposes for collecting and using personal information through its video surveillance and key fob system is the type of space that is under surveillance or monitoring. The Icon buildings are a mix of apartment-style condominiums and townhouses where owners or residents occupy the private

---

[82] Order P09-02, 2009 CanLII 67292 (BC IPC); *Investigation Report P17-01: Use of employee surveillance by a BC chicken catching organization* at pp. 13-14 <https://www.oipc.bc.ca/investigation-reports/2099>; *Audit and Compliance Report P16-01: Over-collected and Overexposed – Video Surveillance and Privacy Compliance in a Medical Clinic* at pp. 21-23 <https://www.oipc.bc.ca/audit-and-compliance-reports/2111>; Order P2006-008, 2007 CanLII 81634 (AB OIPC) at para. 56. See also *The Owners, Strata Plan BCS 435 v. Wong*, 2020 BCSC 1972 at paras. 83-91.

space of their home and collectively share spaces and facilities such as the gym, pool, lobby, hallways, parking garage and elevators.

[126] I am satisfied that a reasonable person would conclude that people generally have a higher expectation of privacy in the common areas of their residential building compared to when they are in a public space such as a retail store, business, workplace or transit facilities. This higher expectation of privacy does not mean it will always be inappropriate for a strata corporation to collect and use personal information through electronic monitoring systems. Privacy is "not an all-or-nothing concept."[83]

[127] Instead, the reasonable person standard under PIPA requires a contextual approach to determining when electronic surveillance is appropriate. It requires organizations to evaluate and ensure that their use of electronic surveillance is appropriate in the circumstances, while taking into account the right of individuals to protect their personal information. This approach is consistent with PIPA's stated purposes which are to recognize both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for appropriate purposes.

Video surveillance – are the purposes appropriate?

[128] As noted, the Organization's purposes for collecting and using personal information from its video surveillance system are for the following purposes:

- To prevent, detect and investigate break-ins and thefts.
- To ensure the safety of the complex owners, tenants, occupants and visitors and provide assistance during health emergencies.
- For bylaw enforcement, including ensuring proper garbage disposal.
- To prevent and investigate damage to strata property.

[129] I will consider below each of the Organization's purposes to determine whether those purposes are "appropriate" in the eyes of a reasonable person based on the circumstances.

Video surveillance to prevent, detect and investigate break-ins and thefts

[130] The Organization submits that one of its purposes for collecting and using personal information through its video surveillance system is for security reasons, primarily to deter and detect break-ins and thefts. The Organization says the

[83] *R. v. Jarvis*, 2019 SCC 10 at para. 41.

video cameras are needed to prevent unauthorized entries through the front lobby doors and parkade gates. The Organization says there were "numerous break-ins through the garage gates" before the cameras were installed.[84] The Organization explains that people would dash in behind cars entering through the garage gates to steal bicycles and break into cars.

[131] The Organization also identified the area around the townhouses as a security concern. It explains that "the townhouse cameras record the area in front of the townhouses that cannot be seen from the street because of the landscaping or other areas of the strata corporation."[85] It says there were "numerous break-ins and attempted break-ins of the townhomes." It describes one incident where someone entered a resident's townhouse and stole some items while the resident was asleep. The Organization says the cameras eliminated incidents in this area for a couple of years.

[132] The Organization also submits that it has a duty to protect the strata's common areas from theft and damage. As an example, the Organization says the cameras deter people from stealing personal items from the change rooms in the pool area and the gym. The Organization says the cameras are needed to protect valuables that residents and their guests "routinely" leave in the pool and fitness room such as wallets, car keys and cell phones.[86] The Organization also says the lobby cameras, front door cameras and the elevator cameras eliminated "numerous incidents where people would sneak into the building through the doors and cause damage."[87]

[133] For the reasons to follow, I am not satisfied that it is appropriate in these circumstances to collect and use people's personal information from the video surveillance system to deter and detect break-ins and thefts. The Organization's evidence falls short of establishing there were legitimate security concerns or incidents, that it first tried or considered other available measures to address these incidents and that the video surveillance system was likely to be effective in resolving or reducing these incidents.

[134] I have reached this conclusion based on the following factors and circumstances:

1) The sensitivity of the information.
2) Manner of collection and degree of intrusiveness.
3) Insufficient evidence to establish legitimate security concerns or threats.
4) Failure to consider or try other available security alternatives.

---

[84] Organization's submission dated August 20, 2018 at p. 1.
[85] Organization's submission dated August 20, 2018 at p. 2.
[86] Letter from organization's lawyer to complainant, dated March 9, 2017 at p. 2.
[87] Organization's submission dated August 20, 2018 at p. 2.

5) Lack of evidence to establish that its security measures are likely to be effective.

[135] I will address these factors and circumstances below in turn.

Sensitivity of the information

[136] The video surveillance system records images that can capture an identifiable individual, their activities, physical appearance and condition. Generally, this kind of information is not as sensitive as, for example, medical or financial information since it is publicly observable by other individuals in the strata's common or shared spaces. However, I conclude the collected images can convey a great deal of information about the filmed individuals such as their personal lifestyle, habits and affiliations.[88] I find the recording of this information over a period of time and the ability to readily review and analyze it makes this method more intrusive than collection by ordinary physical observation.[89]

Manner of collection and degree of intrusiveness

[137] Organizations should limit the collection and use of personal information to only what is needed to achieve the specified purpose. Therefore, an organization that believes video surveillance is an appropriate response to documented security or safety concerns should limit the use and viewing range of cameras as much as possible in order to monitor or record only during the times that meet the organization's specific purpose.[90]

[138] In the present case, I find the degree of intrusiveness is high since the cameras run 24 hours a day, 7 days a week.[91] The continuous collection of this information can have personal and social effects on individuals while they are under surveillance.[92] The video footage is also transmitted through a live feed to a monitor at the concierge desk located in the lobby area. The complainant provided a photo that shows an image of the live monitor feeds.[93] The Organization acknowledges that the live feed from the video cameras assists the concierge with monitoring the exterior doors, the pool and gym areas.[94]

[139] The Organization does not explain why it is not possible or practical to limit the collection and use of personal information to set periods of time when security and safety incidents are more likely to occur or when they have occurred

[88] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60.
[89] Order P09-01, 2009 CanLII 38705 (BC IPC) at para. 119.
[90] OIPC Audit and Compliance Report, P16-01, 2016 BCIPC 56 at p. 10 <https://www.oipc.bc.ca/audit-and-compliance-reports/2111>.
[91] Bylaw 44 found in Organization's submission dated August 20, 2018.
[92] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 60.
[93] Complainant's submission dated September 19, 2018.
[94] Organization's submission dated August 20, 2018 at p. 3.

in the past. I was not provided with any evidence that the Organization assessed and considered limiting when the cameras operate. As a result, I am not satisfied that the Organization's collection and use of personal information is limited to only what is needed to achieve its specified purposes.

[140] I note the complainant claims the lobby surveillance footage is available to residents in real time via channel 69. He provided a tv programming guide which identifies channel 69 as "lobby security cameras."[95] The Organization acknowledges that there was a system that allowed residents to see who was calling them at the front entrance.[96] The Organization explains that this was a system installed by a cable provider at the request of the developer. However, it says the strata council and most people in the building were not aware of it and it was disconnected once discovered.[97]

[141] There was no evidence provided to contradict the Organization's submission that this live video feed was disconnected. If the video feed was still available to residents, then I find it reasonable to conclude that the complainant could have provided some proof that the video feed was still active and available. In the absence of such evidence, I accept the Organization's submission that the front entrance video feed is no longer available to the strata's residents.

Insufficient evidence to establish serious security concerns or threats

[142] A circumstance that I find relevant is that the Organization's video surveillance system was originally installed by the developer.[98] It is common nowadays for most condominium buildings to incorporate and install video surveillance into a building's design. The intent is to use the cameras once the building is completed and occupied. In order P09-02, Adjudicator Fedorak encountered a similar circumstance. He considered whether there was any evidence of legitimate security concerns or threats prior to the implementation of video surveillance, including the number of incidents.[99]

[143] To establish the appropriateness of using video surveillance to ensure security in those circumstances, Adjudicator Fedorak was willing to consider evidence at the time the building was constructed (between 1999 and 2003) that would lead to a reasonable expectation that there would be break-ins at the main entrances.[100] No such evidence was provided by the strata corporation in that

[95] Attached to Complainant's May 27, 2020 submission.
[96] The Organization first refers to this channel as "channel 39" and later said it was "channel 54", but nothing turns on this fact.
[97] Organization's submission dated June 9, 2020 at p. 2.
[98] Organization's submission dated June 9, 2020.
[99] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 64.
[100] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 64.

case and he concluded "there was merely an assumption, as yet unsupported, of any security threat."[101]

[144] I note that strata corporations are not normally formed until after the building is constructed so typically do not have input into the building's security or safety measures. However, once the strata corporation is established, it must assess and justify the appropriateness of its monitoring systems. Where a strata corporation is considering the activation of a video surveillance system as a preventative measure, it must identify and document in writing any potential security or safety risks.

[145] This analysis should identify and assess the existence and extent of those risks, which may take into account neighbourhood crime rates and the verifiable experiences of nearby buildings or residences. It is not sufficient, however, to rely on speculation, assumptions or unsupported anecdotal evidence. Organizations must demonstrate the type of security or safety risks by showing what incidents occurred in the past or are likely to occur in the future.

[146] Furthermore, a strata corporation should be prepared to justify the use of a surveillance system based on verifiable, specific concerns about the personal safety of people living in a strata corporation, or in order to protect personal and common property, that other measures have failed to address.

[147] For example, in 2004, the Federal Court approved the installation and use of video surveillance to monitor the entrances and exits of a Canadian Pacific Railway (CPR) maintenance facility that proved it had suffered 148 incidents of theft, damage, trespass, vandalism and violence over five years.[102] Similarly, in 2006, Alberta's former Information and Privacy Commissioner found that a fitness centre's installation of video surveillance was authorized under that province's private sector privacy legislation.[103] The fitness centre established that there were approximately 900 incidents of thefts in the locker room area in a three-year period.

[148] In this case, the Organization provided no evidence as to what circumstances led it to initially activate and use the video surveillance system installed by the developer. However, it does provide some thoughts about the current circumstances. The Organization says the Icon buildings are located in downtown Vancouver and its security measures were taken to protect the strata property and the strata owners.[104] It explains that "living in the middle of a large

[101] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 64.
[102] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII).
[103] Order P2006-008, 2007 CanLII 81634 (AB OIPC).
[104] Organization's submission dated August 20, 2018 at p. 1.

city and in a large shared community requires methods you may not need to use in a private residence and most of our owners understand this."[105]

[149] I assume the organization is arguing that the buildings are located in a high crime area. If so, I acknowledge that the surrounding neighbourhood or the location of the strata building may be a relevant factor for the implementation of video surveillance systems. However, the Organization did not provide sufficient evidence or explanation to assist me in understanding the level of crime in that particular area.

[150] The Organization quantifies the security concerns as "numerous" incidents and break-ins and describes one specific incident of a townhouse break-in. However, it does not provide information regarding these "numerous" incidents; nor does it provide evidence to support its claims such as security records or incident reports created at the time. The Organization also says the cameras deter people from stealing personal items from the change rooms in the pool area and the gym. However, it does not provide any detail or evidence about the thefts that occurred in that area.

[151] Therefore, based on the materials before me, there is insufficient information and evidence for me to determine the severity, frequency or number of incidents to justify the implementation and use of video surveillance to deter and detect break-ins and thefts. The Organization's general claims and limited examples do not establish that the security concerns were serious and frequent enough that it was appropriate to collect and use personal information through a video surveillance system for those purposes.

Other available security alternatives to video surveillance

[152] PIPA does not explicitly prohibit the use of video surveillance by strata corporations, but because of their "arbitrary invasiveness", video surveillance systems should only be used after less privacy-intrusive measures have failed to address a serious problem.[106] Organizations must first assess whether there are less intrusive methods to achieve the intended purpose without the use of video surveillance.

[153] In terms of alternative measures, the Organization says that it posted signs and issued reminders to residents regarding concerns with the parkade gates, lobby, elevator, gym and pool area, townhouse and courtyard area and garbage room. It also explained that there was a concierge in place who conducted regular security patrols before the upgrade of the existing cameras and the installation of the two new cameras. The Organization says none of

[105] Organization's submission dated October 4, 2018 at p. 4.
[106] Investigation Report P98-012, *Video Surveillance by Public Bodies: A Discussion*, March 31, 1998 at p. 14, <https://www.oipc.bc.ca/investigation-reports/1259>.

these measures fixed the problems and since the security upgrade, it has had "significantly fewer security incidents."[107]

[154] For the parkade gates, the Organization describes how it tried to mitigate the break-ins by posting signs or notices on the parkade gates, in the elevators, on mail room bulletin boards and in the strata meeting minutes. It says that it required residents using the parkade gates to stop and wait for the gates to close, but those measures were ineffective since not everyone followed those instructions.

[155] The complainant submits that the Organization failed to provide tangible evidence or proof of what steps it first took to mitigate its security concerns and how those methods failed.[108] The complainant says the Organization's examples do now show what other methods it first tried to address its security concerns. He also claims the Organization's concerns about the gym and pool area and garbage room are about minor bylaw enforcement and not security concerns.

[156] I am not persuaded by the Organization's evidence that it first considered other available alternatives or tried other less privacy-intrusive measures before resorting to video surveillance. The Organization says its unsuccessful measures involved issuing notices to residents and conducting regular security patrols. The Organization does not explain why it did not consider or try other obvious security alternatives such as increasing security personnel, installing or upgrading alarm systems, reinforcing gates, doors and windows and even better lighting.

[157] The strata council minutes provided by the complainant also demonstrate the Organization did not wait to first try alternative measures before employing video surveillance. It was using the video surveillance system at the same time it was trying other countermeasures. For example, the January 2016 meeting minutes establish the Organization was adding extra security hardware and limiting access times to the bicycle storage room and looking into accelerating the closing cycle times for the parkade gates.[109] I note that the Organization was implementing or considering these measures after the video surveillance system upgrade in 2015. As a result, it is not apparent that the Organization first tried other unsuccessful measures to address its security concerns before resorting to video surveillance. Instead, the evidence indicates that the Organization was using or considering other security measures even after the upgrade of the video surveillance system.

[158] For the two new cameras, the Organization says it installed a camera around the townhouse area in response to numerous break-ins. It explains that the landscaping in front of the townhouses provides a great place for intruders to

[107] Organization's submission dated August 20, 2018.
[108] Complainant's submission dated September 19, 2018 at pp. 9-10.
[109] Complainant's submission dated June 24, 2020.

hide from view while breaking into a townhouse. The strata council meeting minutes show that, in February 2015, the Organization was considering improving the lighting in the townhouse area. There is no evidence or explanation though as to whether improved lighting was implemented in this area and the effectiveness of this technique. It is further unclear whether the Organization first tried to address its security concerns by focusing on the landscaping issues in front of the townhouses.

Effectiveness of video cameras in addressing the security threats or concerns

[159] The complainant submits that the Organization failed to provide tangible evidence or proof of how the surveillance system has improved or addressed the security concerns.[110] The complainant contends that the video surveillance system does not deter crime. The complainant questions how a security camera stops someone from entering a building or stops an aggressive person.

[160] The complainant also submits that video surveillance footage may not always prove effective in identifying the person responsible. He claims the biggest robbery in the building's history happened just after the system was installed and several bikes were stolen. He says the strata council reported that the person stealing the bikes was not identifiable from the video footage. The complainant cites this incident as an example of how the surveillance system is "not a useful tool for security as it is not a deterrent for crime and when crime happens it is not useful for apprehending the culprit(s)."[111]

[161] The Organization disputes the complainant's allegations and claims the video cameras were effective in addressing its security concerns. The Organization says that, since the "installation" and upgrade of the video surveillance cameras, it has had "significantly fewer security incidents."[112] However, I agree with the complainant that there is a lack of correlating evidence to support the Organization's perceived resolution or reduction of the security incidents.

[162] The Organization quantifies the number of security incidents as "numerous" and says there were "significantly fewer" incidents after the security upgrade. However, it does not provide any supporting evidence, such as a security review or audit, to assist in establishing the effectiveness of the video surveillance in reducing the security incidents. The Organization had several opportunities to respond to the complainant's arguments about the lack of "tangible evidence and proof", but did not provide sufficient supporting evidence

[110] Complainant's submission dated September 19, 2018 at pp. 9-10.
[111] Complainant's submission dated May 27, 2020.
[112] Organization's submission dated August 20, 2018 at p. 3.

to establish the likely effectiveness of its video surveillance system in addressing the "numerous" security incidents.

[163] In contrast, the Alberta fitness centre in Order P2006-008 saw a decline from 900 incidents in a three-year period to just 10 thefts in a two-year period after the installation of the security cameras.[113] Likewise, the CPR railyard who installed video surveillance cameras at its maintenance facility established there was a decline from 148 incidents in a five year period to no incidents since the video cameras were installed.[114] In the absence of statistics or analysis from the Organization, I am unable to determine on an objective basis whether there was a decline in the security incidents following the implementation and use of video surveillance.

[164] As to the effectiveness of the upgraded cameras, the January 2016 strata council meeting minutes shows the Organization was using or considering other security measures even after the upgrade of the video surveillance system in 2015. For example, the January 2016 meeting minutes establish that additional security measures were implemented to address recent vandalism and attempted break-ins of the bicycle storage rooms.[115] It is unclear why the Organization would need to employ other security measures if the upgraded video surveillance was successful or likely to be effective in addressing the Organization's security concerns.

Summary on video surveillance to deter and detect break-ins and thefts

[165] It may be appropriate in some circumstances for a residential strata corporation to use video surveillance for security purposes, but that determination will always depend on the facts of the specific case.[116] To justify employing a video surveillance system to collect personal information for such a purpose, an organization must prove there were legitimate security incidents or concerns, that it considered or tried other available, less-privacy intrusive alternatives before resorting to video surveillance and that the video cameras were likely effective in resolving or reducing these incidents. For the reasons given above, the Organization's submissions and evidence falls short of establishing these requirements. Despite having several opportunities to provide additional submissions, the Organization did not provide sufficient explanation or evidence to establish that it was appropriate in these circumstances.

[166] I am aware of Alberta Order P2016-02 where the adjudicator considered whether a condominium corporation's use of video surveillance cameras complied with ss. 11 (collection) and 16 (use) of Alberta's PIPA. Sections 11 and

[113] Order P2006-008, 2007 CanLII 81634 (AB OIPC) at para. 67.
[114] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII) at para. 179.
[115] Complainant's submission dated June 24, 2020.
[116] For example, Order P09-02, 2009 CanLII 67292 (BC IPC).

16 of Alberta's PIPA provide that an organization may collect and use personal information "only for purposes that are reasonable" and "only to the extent that is reasonable for meeting the purposes" for which the information is collected or used. Section 2 of Alberta's PIPA says that in determining whether a thing or matter is reasonable or unreasonable, the standard to be applied is "what a reasonable person would consider appropriate in the circumstances."

[167] The adjudicator in Order P2016-02 was satisfied the evidence established that it was reasonable for the condominium corporation to install surveillance cameras "to maintain the security of the condominium, at the direction of the owners."[117] But, each case obviously turns on the evidence before the decision-maker. Furthermore, the adjudicator's reasons regarding collection and use in Order P2016-02 lacks explanatory detail in terms of the assessment of the evidence in that case.

[168] The adjudicator also does not appear to have taken a contextual approach as previous Alberta and BC orders have done in determining whether the purposes for the collection or use of personal information was appropriate in the circumstances.[118] As a result, I find Order P2016-02 is of no assistance in determining whether the Organization's collection and use of personal information through its video surveillance system for security purposes was appropriate in this case.

Video surveillance to ensure safety and provide assistance during health emergencies

[169] The Organization submits that it has a duty to protect the people who use the strata's common areas. The Organization says the concierge does regular patrols of the common areas as part of the strata's total security plan, but video surveillance is needed to address safety concerns in the building. The Organization says the residents have expressed concerns for their safety when they use the gym and pool since there is no lifeguard and most often there is only one person using these facilities.

[170] The Organization explains that the cameras allow the concierge to monitor multiple areas and to provide residents with aid when necessary, specifically emergency aid in the pool and gym area. The Organization describes the cameras in the gym and pool as "equipped with wide angle lenses that allow the cameras to see the external doors and portions of the inside of each of those areas."[119] The Organization describes three incidents where the concierge's live monitoring of those areas addressed safety concerns by assisting a resident who was suffering a heart attack, stopping a couple from inappropriate behaviour in

[117] Order P2016-02, 2016 CanLII 11214 (AB OIPC) at para. 50.
[118] For instance, Order P2006-008, 2007 CanLII 81634 (AB OIPC) at para. 56.
[119] Letter from organization's lawyer to complainant, dated March 9, 2017 at p. 3.

the hot tub and decreasing the threatening actions of a person in the gym towards women.[120]

[171] The Organization claims that, "since the cameras were installed, the number of incidents has decreased dramatically."[121] The Organization says these areas are only monitored by the concierge and the strata council does not view the tape unless "it is something of great importance" and even then it would only be the strata president or someone appointed by council in the strata president's absence.[122]

[172] The complainant challenges the appropriateness of the Organization's collection and use of personal information through the cameras in the pool and gym area. The complainant says the Organization's examples are not security concerns, but are examples of rule or by-law infractions.[123] The complainant also notes the Organization's submissions do not show what other unsuccessful methods were first tried by the Organization.

[173] The complainant submits that extended building patrols by a security guard or the concierge may be an alternative solution not fully utilized by the Organization. In particular, the complainant alleges the concierge has stopped patrolling in favour of live video monitoring. The complainant also believes the Organization contradicts itself in its submissions because the Organization is arguing that they use the cameras to monitor these facilities, but that recordings are not viewed by authorized individuals unless it is something of great importance.

> *Is this collection and use of personal information by video cameras appropriate in the circumstances?*

[174] Before installing video equipment or activating a surveillance system that was installed by the original developer, a strata corporation should be prepared to justify its use based on verifiable, specific concerns about the personal safety of people living in a strata corporation. A reasonable person would consider it appropriate to collect and use personal information obtained through video surveillance where there is evidence that physical safety is a legitimate issue that can most effectively be addressed through video surveillance.[124]

[175] In Order P09-02, Adjudicator Fedorak found the strata corporation failed to provide enough evidence to show there was a safety risk associated with its pool

---

[120] Organization's submission dated August 20, 2018 at p. 2.
[121] Organization's submission dated August 20, 2018 at p. 2.
[122] Organization's submission dated August 20, 2018 at p. 3.
[123] Complainant's submission dated September 19, 2018 at p. 10.
[124] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 76.

that could only be addressed effectively through video surveillance.[125] In reaching this conclusion, he found there were no reported incidents of injury in the pool area. He also assessed the effectiveness of the video surveillance in addressing the safety concern and concluded that it was unclear how a video camera would stop someone from diving into a shallow pool. He also noted that many pools in other buildings do not have a lifeguard or video surveillance. In terms of alternative measures, Adjudicator Fedorak found there was no evidence that the warning notices routinely seen in swimming pools would not suffice to warn individuals of danger.[126]

[176] In the present case, I am not satisfied that physical safety is a legitimate issue for which it would be appropriate to use video surveillance. The Organization provided no supporting evidence that the residents of the Icon buildings are concerned with their safety while on strata property or in the pool and gym area so that real-time video monitoring is appropriate. I also note that the video cameras operate continuously; therefore, there needs to be evidence of legitimate and verifiable safety concerns to justify the high intrusion of privacy in these more sensitive areas where residents and guests are in their workout clothes or swimsuits.

[177] As for the type of safety concerns that the Organization seeks to address, it is not apparent to me and the Organization does not explain how preventing inappropriate behaviour in the hot tub or in the pool area is a personal safety concern. The Organization only says "the camera prevented what could have been a traumatic incident for young children" who may have entered the pool area at the relevant time.[127]

[178] In terms of effectiveness, the Organization did not explain how its recorded video footage would assist with providing immediate assistance or emergency aid to someone who is being assaulted or experiencing a heart attack. The video footage would likely only capture the event after it has occurred and, therefore, would not be effective in allowing the Organization to meet its objective of ensuring safety and providing assistance during health emergencies throughout the strata complex.

[179] Furthermore, I agree that heart attacks and drownings are safety concerns; however, I am not persuaded that live video monitoring is likely to be an effective way to address these concerns. The Organization says the concierge's live monitoring assisted a resident who was suffering a heart attack in the gym, but it is not clear whether the Organization means the concierge administered first aid or called emergency services. Nevertheless, to provide immediate and effective emergency aid from heart attacks or drownings, the

[125] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 76.
[126] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 74.
[127] Organization's submission dated August 20, 2018 at p. 2.

concierge would be required to continuously monitor the entire strata complex, including the gym and pool area while it is in use, and may also require training in life-saving techniques. The Organization did not provide any supporting evidence to show that the necessary resources and skills are in place to make this a realistic objective.

[180] I am also not satisfied the Organization tried or considered other reasonable alternatives to address its safety concerns. Organizations should only use video surveillance after other less privacy intrusive measures to achieve their purposes have been considered or exhausted.[128] The Organization does not discuss what other measures were first used or contemplated and why those actions were unsuccessful or not viable. For instance, the Organization does not explain why other safety measures commonly used in private recreational facilities would not suffice such as proper signage, providing safety and first aid equipment or an emergency call button.

[181] For the reasons given, I find the Organization has not demonstrated that there is a safety risk associated with the strata complex, particularly the pool and gym areas, that can most effectively be addressed through video surveillance. As a result, I am not satisfied that a reasonable person would consider it appropriate for the Organization to collect and use personal information through a video surveillance system for the purpose of ensuring safety and providing emergency aid throughout the strata complex.

Video surveillance for bylaw enforcement

[182] The Organization says that it uses footage from the video surveillance system to investigate and confirm bylaw infractions.[129] The Organization claims that it is duty bound under the *Strata Property Act* to enforce its bylaws, including conducting an investigation as to whether a bylaw was contravened and the collection of fines or the recuperation of its costs through the Civil Resolution Tribunal process.

[183] The Organization provided some examples of bylaw enforcement such as inappropriate behaviour in the pool area involving several adults and the monitoring of the parkade gates to ensure residents wait for the gates to close to prevent unauthorized entry.[130] The Organization also confirms the complainant was investigated for violating a bylaw that prohibits the installation of heaters on a unit's balcony when the heating device is installed through the building's structure.[131]

---

[128] OIPC Audit and Compliance Report, P16-01, 2016 BCIPC 56 at p. 10 <https://www.oipc.bc.ca/audit-and-compliance-reports/2111>.
[129] Organization's submission dated August 20, 2018 at p. 3.
[130] Organization's submission dated October 4, 2018 at pp. 2-3.
[131] Organization's submission dated June 9, 2020 at pp. 1-2.

[184] The Organization also submits the garbage room cameras helped with ensuring and enforcing proper garbage disposal. It explains that, over the years, the garbage rooms have been problematic with people leaving all kinds of junk such as toilets and old barbeques, household items and used furniture. It says residents were also not paying attention to the rules around recycling and the disposal of dangerous materials. The Organization says the discarded items were health hazards and the strata corporation incurred a significant cost to have these items removed.

[185] The Organization states that it tried other unsuccessful measures to address the garbage room concerns such as putting up signs and issuing reminders in its meeting minutes for residents to deal with their garbage in a safe and sanitary manner. However, it says none of those measures seemed to fix the problems. The Organization says the video cameras have resolved the improper dumping in the garbage rooms and it is "remarkable how clean these areas have become."[132]

[186] The Organization also claims the video footage allowed them to protect residents from aggressive dogs in the elevator and lobby areas. It says there were "a number of times where there have been aggressive or vicious dogs in the elevator or lobby scaring people" and that it was able to deal with the dog owners and protect its residents through the use of cameras.[133]

[187] The complainant says the Organization is also using video footage to catch people committing infractions such as using a personal trainer in the gym, failing to wait for the overhead parkade gate to close completely before driving away and littering in the parkade. He also alleges the Organization used video footage to identify potential violations of a bylaw that prohibits short-term accommodation. The complainant claims staff confronted and questioned a guest, and himself on a separate occasion, after seeing them with luggage on video surveillance.[134] The complainant believes he and his guests were monitored through the video surveillance system even though there was no corresponding complaint.

[188] In response to the complainant's allegations, the Organization asserts that it does not have anyone watching the video footage for the specific purpose of finding bylaw infractions. In particular, the Organization says concierge staff do not scan the video monitors looking for short-term vacation renters since "they are quite apparent when they come in the door."[135]

---

[132] Organization's submission dated August 20, 2018 at p. 3.
[133] Organization's submission dated August 20, 2018 at p. 2.
[134] Complainant's submission dated May 27, 2020 at p. 2.
[135] Organization's submission dated October 4, 2018 at p. 2.

[189] The Organization says the concierge or strata council president will only review the video images if someone has complained of a bylaw infraction and it needs to conduct an investigation. It explains that some residents will ask for proof when they are sent a warning letter of a bylaw infraction and the Organization can supply this proof through the video footage. The Organization says if an owner requests proof of a bylaw infraction they will only be shown the part of the video that relates to them.

Is the Organization using video cameras to collect and use personal information for bylaw enforcement?

[190] Based on the parties' submissions, I conclude the Organization is collecting personal information through its video surveillance system for the purposes of bylaw enforcement. The Organization acknowledges that it collects and uses footage from the video surveillance system to investigate, confirm and enforce bylaw infractions. However, the parties disagree about what bylaws or rules are being enforced through the use of video surveillance.

[191] I was not provided with a full copy of the strata's bylaws to assist me in verifying all the specific provisions at issue. However, the parties' submissions and evidence indicate the Organization has bylaws prohibiting the use of strata units for short-term accommodation and improper garbage disposal.[136] The Organization may also have bylaws regulating pet behaviour and the behaviour of residents and guests in the strata's common areas.

[192] I also conclude the Organization has a bylaw restricting residents from installing a heating device on a strata unit's balcony when it is connected to the structure of the building. Both parties do not dispute that the complainant was investigated for this bylaw contravention and that footage from the video surveillance system was used as part of the investigation and enforcement. My own review of the relevant email and its attachments confirms these events.

[193] However, the Organization denies the complainant's allegation that it used video surveillance to enforce its bylaw prohibiting short-term accommodation. The Organization says its concierge identified a resident of a unit that was running an Airbnb based on the variety of people coming and going from the suite, from an online posting on a website and from their conversation with an individual carrying a suitcase who admitted to being an Airbnb guest.[137]

[194] The Organization also denies using the surveillance footage to identify an individual who used a personal trainer in the gym. The Organization says the concierge identified this person and the alleged bylaw infraction from personal observation. It explains the concierge noticed the person sitting in the lobby

[136] The complainant provided a copy of one page from the strata's bylaws (page 7 of 30).
[137] Organization's submission dated June 9, 2020 at p. 2.

waiting for their personal trainer and that this individual was someone who kept a fob to use the gym even though they had moved out of the building.[138]

[195] Based on the materials before me, I am not satisfied the Organization is collecting personal information from its video surveillance system for the purpose of enforcing its bylaw prohibiting short-term accommodation and its gym usage bylaws. I understand the complainant strongly believes the Organization is doing so; however, the Organization's explanations are reasonable and there is not enough evidence before me to contradict this information.

[196] Therefore, I am satisfied that the Organization is collecting and using footage from the video surveillance system to investigate, confirm and enforce its bylaws regarding garbage disposal, pet behaviour and the installation of a heater on a balcony, but not for enforcing its bylaw prohibiting short-term accommodation and its gym usage bylaws.

> *Is this collection and use of personal information by video cameras appropriate in the circumstances?*

[197] The collection and use of personal information through video surveillance for bylaw enforcement was an issue in two previous orders.[139] In Order P09-02, several residents of a strata building complained their strata corporation was using video footage to enforce bylaws such as dress code violations, smoking or drinking in prohibited areas and allowing dogs to walk into the building instead of carrying them.

[198] In that case, Adjudicator Fedorak found the strata corporation did not provide sufficient evidence to establish that the bylaw violations at issue, whether minor or serious, had become a legitimate problem that required video surveillance as a means of enforcement.[140] For instance, he found in those circumstances that the reasonable person standard did not support the collection and use of video surveillance footage for minor bylaw violations such as a dress code bylaw and the improper moving of furniture through the lobby.

[199] In applying the reasonable person standard, Adjudicator Fedorak also considered whether the system was implemented in a way that minimized the privacy intrusion to only what was necessary to achieve the strata's purposes. He noted that most of the camera footage in that case was routinely reviewed the following day, even if there was no reported incident or complaint. He found it

---

[138] Organization's submission dated October 4, 2018 at p. 2.
[139] Order P09-02, 2009 CanLII 67292 (BC IPC) and Order P2016-02, 2016 CanLII 11214 (AB OIPC).
[140] Order P09-02, 2009 CanLII 67292 (BC IPC) at paras. 80 and 88.

was inappropriate for the strata to conduct a daily pre-emptive review of the video footage, including for the purposes of identifying bylaw infractions.[141]

[200] In the present case, I am satisfied that improper garbage disposal had become a legitimate problem that required video surveillance as a means of enforcement. I accept that people were leaving all kinds of junk and hazardous materials in the garbage rooms, which required the Organization to spend a significant amount to remove and properly dispose of those items.

[201] I also accept the Organization was unsuccessful in addressing the garbage room concerns by putting up signs and issuing reminders to residents. It is not apparent what other alternative measures the Organization could have used since improper dumping is likely to occur at all times and when there is no one to witness the incident.

[202] In terms of effectiveness, the Organization says the original cameras were "outdated, cheap and ineffective" and were not a deterrent since "the resolution was [too] low and it was extremely difficult to identify anyone on them."[142] The Organization says the upgraded cameras have resolved the improper dumping in the garbage rooms.[143] I accept the upgraded video cameras were likely a deterrent to individuals who intend to improperly dispose of their garbage. I also note that the complainant does not contradict what the Organization says about the effectiveness of the video cameras in addressing the issues around improper garbage disposal.

[203] With regards to the retention of the recorded video footage for the purposes of enforcing its garbage disposal bylaw, I find the Organization's retention policy to be appropriate. The Organization's retention policy is identified in Bylaw 44, which states video footage recorded and collected by the Organization is normally stored for a period of "up to one month from the date of recording."[144] However, the Organization's representative in this inquiry says the video footage is stored for 10 days and automatically deleted.[145] The Organization does not explain this inconsistency and whether there was a change in policy.

[204] Nevertheless, without evidence to the contrary, I conclude that a 10 day retention period is more reasonable than a one month period. For instance, I find it reasonable to conclude that any incidents of improper garbage disposal can usually be discovered within one or two days. Further, one week is typically more than sufficient for the Organization to make a decision whether it is necessary to

---

[141] Order P09-02, 2009 CanLII 67292 (BC IPC) at paras. 82-83.
[142] Organization's submission dated August 20, 2018 at p. 4.
[143] Organization's submission dated August 20, 2018 at p. 3.
[144] Bylaw 44 found in Organization's submission dated August 20, 2018.
[145] Organization's submission dated August 20, 2018 at p. 3.

retain the footage past the normal retention period in order to further investigate an incident or use the footage as evidence. Bylaw 44 notes that the storage period may be extended for those files required for bylaw enforcement purposes. I find it reasonable that a longer retention period may be necessary on occasion for investigative or enforcement purposes.

[205] I do not, however, find it is appropriate for the Organization to use video surveillance to enforce bylaws other than the garbage disposal bylaw. From the Organization's submissions, there appears to be an unspecified number of aggressive dog encounters and parkade gate incidents, one unauthorized heater installation and one or two occurrences of inappropriate behaviour in the pool and hot tub area. These type of bylaw infractions do not appear severe enough in nature to justify the Organization's recording and live monitoring of residents and guests through video surveillance. The Organization also does not specify when all of these incidents occurred for me to assess the frequency of these events and the examples provided seem limited in number, considering the approximately 15-year history of the two Icon buildings.

[206] It is also unclear that the Organization considered or tried other alternative, reasonable measures of bylaw enforcement before resorting to video surveillance. Except for signage and reminder notices, the Organization does not sufficiently identify what other measures it considered or tried to deter prohibited behaviour or gather information about potential bylaw contraventions. The Organization does not explain why eyewitness accounts or other alternative measures are not feasible or appropriate. I note that most of the alleged bylaw violations it mentions appear to have witnesses who could have provided the necessary evidence to identify the responsible individuals. Further, from the Organization's submissions, the concierge appears quite proficient at spotting bylaw infractions.

[207] The Organization also says the footage is only viewed when there is a complaint; however, I conclude this is not accurate as the Organization says the concierge used the live video feed to "spot" and "stop" inappropriate behaviour in the hot tub.[146] As a result, I am not satisfied that the collected personal information is only viewed upon receipt of a complaint. Similar to Order P09-02, I find it inappropriate for the Organization to use the live video feed or the recorded video footage to monitor for bylaw infractions without a reported incident or complaint.

[208] In terms of effectiveness, I acknowledge that video footage may be effective or conclusive proof that an individual violated a bylaw about dogs, heater installation or pool etiquette; however, the privacy intrusion is high. The cameras run 24 hours a day, 7 days a week so images are being collected of

[146] Organization's submission dated August 20, 2018 at p. 2.

people who may be committing bylaw contraventions, along with those residents or guests who are complying with the bylaws and rules.

[209] Considering all the relevant circumstances, I conclude that a reasonable person would find the Organization's collection and use of personal information through its video surveillance system to enforce its bylaws regarding garbage disposal to be appropriate. However, for the reasons given, I am not satisfied that it was appropriate for the Organization to do so for the enforcement of its other bylaws.

Video surveillance to prevent and investigate property damage

[210] The Organization submits that it also uses video surveillance because it has a duty to protect the strata's common areas from damage.[147] It describes two separate incidents of drivers plowing into the parkade gates and one incident where an individual kicked holes in the gym walls.[148] The Organization says this is not an exhaustive list, but are examples of more serious incidents.[149]

[211] The Organization says the level of damage to the parkade gates was significant, but there was no evidence about the extent of damage to the gym walls. The Organization also did not identify any other areas of the strata complex which suffered, or are likely to suffer, accidental or intentional damage. In terms of effectiveness, the Organization says the footage from the video surveillance system allowed it to identify the individuals responsible for damaging strata property and recover some of its repair costs.

[212] I accept there may be a legitimate issues in the parkade area which require the use of video surveillance, but not for the rest of the strata complex. I recognize that two incidents is a small number of property damage incidents in the parkade area considering the approximately 15-year history of the building. However, the extent of the damage was significant in one instance. I conclude significant property damage constitutes a legitimate issue to justify the use of video surveillance in the parkade area, even though the number of instances is low.

[213] In terms of effectiveness, I accept the video footage from the parkade cameras allowed the Organization to identify the responsible individuals and hold them accountable for the property damage. The Organization also says it "eliminated" these problems with the video cameras.[150] It is also reasonable to conclude that the video cameras act as a deterrent to individuals who intend to

[147] Organization's submission dated October 4, 2018 at p. 3.
[148] Organization's submission dated August 20, 2018 at p. 2.
[149] Organization's submission dated August 20, 2018 at p. 1.
[150] Organization's submission dated August 20, 2018 at p. 2.

commit intentional damage in the parkade area. The possibility of identification would discourage most people from wilfully damaging strata property.

[214] However, it is unclear how the presence of video cameras would prevent accidental damage. The Organization does not explain how the video cameras could change the behaviour of a person who does not intend to cause damage. Nevertheless, I find it appropriate for the Organization to be proactive in safeguarding the parkade area from damage and for ensuring that when it does happen, there may be some evidence that would assist in holding the responsible individuals accountable.

[215] The Organization does not discuss what alternative measures it considered or tried before resorting to video surveillance in the parkade area. However, it is unclear what other method the Organization could have used to effectively identify the responsible individuals. One of the accidental parkade incidents occurred late at night when there were few people around to witness the incident; therefore, eye witness accounts will not always be an available option.

[216] Furthermore, the concierge is only located in the Icon 2 building and cannot reasonably be expected to continuously patrol the parkade areas in both Icon buildings for incidents of vandalism or accidental damage. Even if security patrols were increased, these patrols would not be as effective as video surveillance since there would be gaps in coverage and room for human error or inattention.

[217] I also accept that it would be counter-productive to limit the days and times when the video cameras operate since property damage can occur at any time. As noted, one of the parkade gate crashing incidents occurred late at night. As well, for the reasons given previously, I do not find the Organization's initial 10-day retention policy and its longer retention of the video footage for investigative purposes to be inappropriate. Further, I find the parkade area is not a privacy-sensitive area. Therefore, I am satisfied that using video cameras for the purpose of preventing and investigating property damage in the parkade is appropriate in the circumstances.

[218] However, I find otherwise for the video cameras located in the gym, swimming pool and hot tub areas where residents and guests are in their workout clothes or swimsuits. In these more private areas, I find it reasonable to conclude that residents and guests would consider it more privacy intrusive to have their actions recorded or monitored in real time with a direct video feed to the concierge's desk.

[219] In addition, there was insufficient evidence to show that property damage was a legitimate issue or concern in the gym, swimming pool and hot tub areas.

The Organization describes one incident where a person caused damage to the gym walls; however, there was no evidence about the extent of the damage, or the likelihood that it would happen again. Therefore, I find the Organization did not establish video surveillance was an appropriate response to a single incident of property damage in the gym area.

[220] As a result, for the reasons given, I am satisfied it was appropriate in the circumstances for the Organization to collect and use personal information by video surveillance for the purpose of preventing and investigating property damage in the parkade area, but not in other areas of the strata complex. This finding is consistent with Order P09-02, where Adjudicator Fedorak found that a reasonable person would consider it appropriate to collect and use personal information obtained through video surveillance where there is evidence that property damage is a legitimate issue that can most effectively be addressed through video surveillance.[151]

Key fob system - are the purposes appropriate?

[221] The Organization submits that it is reasonable and appropriate for it to collect and use personal information from its key fob system for security purposes. As noted previously, the Organization collects information from the key fob readers that is then linked to a computerized database that records each fob use. This linked information identifies the location, date and time of use and the person associated with that fob number. The Organization submits that this collected personal information is needed to control and monitor access to the strata property.

[222] The Organization also collected and used personal information from the strata unit owners and residents to compile and maintain a fob inventory. The Organization collected this personal information by requiring residents and owners to complete a form identifying their name, strata unit number, their fob number, the number of fobs in their possession and whether they were an owner, agent or tenant of the strata unit.

[223] The complainant alleges the Organization is inappropriately using the collected information in the key fob database to investigate and enforce a bylaw that prohibits short-term accommodation, including denying residents access to their units via the elevator.

[224] I will examine each of the Organization's key fob-related purposes below and consider the complainant's allegations regarding the Organization's use of personal information for bylaw enforcement.

[151] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 76.

Using the key fob system to monitor access

[225] The Organization says the personal information collected from the key fob system is needed "to monitor access to the building by bona fide owners and residents, including elevators, which provides a significant level of security for owners and residents."[152] The Organization says the key fobs allow residents to only access the strata's common areas and the floor they live on. With the way the fobs are programmed, the Organization says it prevents an intruder from being able to roam the entire building searching for units to break into. The Organization believes that its key fob system is "the least intrusive way for residents to have access to areas without having the general public have access."[153]

[226] I also note that the Organization relies on Bylaw 44 in support of its position. Bylaw 44 says the following with regards to the Organization's collection and use of the key fob records:

> 44 (2) The Strata Corporation collects data with respect to the usage of each security fob programmed for use at Strata Plan BCS1964.
>
> 44 (3) The video files and/or security fob usage records will be used by the Strata Corporation for surveillance and monitoring purposes only, including the following purposes:
>
> a) being alerted to the presence of trespassers on the strata plan;
> b) preventing, recording, investigating and obtaining evidence of any theft, vandalism, nuisance or damage caused by any person on the strata plan;
> c) ensuring the safety of the complex owners, tenants, occupants and visitors; and
> d) enforcing those Strata Corporation bylaws and rules which relate to theft, vandalism, nuisance or damage caused by any person on the Strata Plan; the safety and security of the strata plan and the complex owners, tenants, occupants and visitors.

[227] The complainant believes the current key fob system is more invasive than the previous system which he says was anonymized. The complainant says the current system allows the Organization to track and monitor every use of the fob in real time using the computers at the concierge desk. The complainant objects to the Organization recording or watching each key fob use and submits the Organization has not proven that it considered less intrusive ways to achieve its purposes.

---

[152] Letter to complainant from Organization's legal counsel dated March 9, 2017 at p. 3.
[153] Organization's submission dated August 20, 2018 at p. 3.

[228] The complainant provided a photo of a computer monitor that he says shows in real time when a key fob is being used, to whom it is registered, and the date, time and location of use.[154] The picture indicates each fob use is a separate entry on a spreadsheet highlighted in green or red. The complainant says a green highlighted entry indicates a successful fob swipe and a red highlighted entry shows an unsuccessful fob swipe.[155] The Organization did not dispute the complainant's account of this real time monitoring and the information that is collected.

[229] In response, the Organization says it is not prepared to anonymize the current system since it allows the Organization to monitor access to the building and the elevators.[156] It believes this monitoring provides a significant level of security for owners and residents. The Organization also claims the current system cannot be changed to anonymize the identity of the fob users, but it did not explain why this is not possible. The Organization also does not explain how its previous key fob system functioned or what it understands the complainant means by an anonymized key fob system.

> *Is collecting and using personal information obtained through the key fob system appropriate in the circumstances?*

[230] I am not satisfied that a reasonable person would find the Organization's collection and use of personal information from the key fob system to be appropriate in the circumstances. The information collected about a resident's key fob usage is not as revealing as images collected from the video surveillance system (e.g. personal physical characteristics are not collected). However, this information reveals a person's movement into and throughout the strata property and may capture their activities such as the use of the pool, gym and the building's other amenities.

[231] Further, I find the degree of intrusiveness is high. The information from the key fob system is collected 24 hours a day, 7 days a week and usually retained for a period of up to ten days from the date of recording. Similar to video surveillance, the storage and reviewability of this information is more intrusive than physical observation since it can reveal a person's location and activity over a period of time. As well, the key fob usage information is not only recorded in a database, but real time usage is visible on a monitor at the concierge desk located in the lobby area. The Organization does not explain why active monitoring is appropriate to achieve its purposes.

[232] In terms of alternative measures, the Organization does not adequately explain how its system of recording and visually monitoring key fob usage on the

---

[154] Complainant's submission dated September 19, 2018.
[155] Complainant's submission dated September 19, 2018.
[156] Letter to complainant from Organization's legal counsel dated March 9, 2017.

concierge's computer monitor works and whether the system allows for a less privacy intrusive way to fulfill its purposes. For instance, the Organization does not sufficiently explain whether the key fob system can be programmed to allow access without generating a usage log in a database or allowing it to be viewed on the concierge's computer monitor. There is no indication that the Organization considered reducing or limiting the amount of personal information that is collected or recorded.

[233] Furthermore, it is unclear how collecting data about a key fob's location and activity would be effective for achieving the Organization's security purposes. The Organization's submission on this issue is vague and lacking in detail. The Organization says Bylaw 44 is a "complete answer" to the reasonable purpose requirements of s. 11.[157] However, the Organization does not explain how the recording and real time monitoring of a key fob's movement throughout the strata property is effective in achieving the purposes identified in Bylaw 44. For instance, it is not clear how collecting key fob usage would indicate the presence of trespassers. There is no information about how the Organization identifies and responds to unauthorized users.

[234] The Organization also suggests that it is collecting personal information from the key fob system to assist the police. It says the key fob system "helps police figure out where an intruder got access to the building."[158] However, this is the full extent of the Organization's submission and it does not provide an adequate explanation of this purpose. Therefore, based on the materials before me, I am not satisfied that collecting personal information for this purpose would be appropriate in the circumstances.

[235] I note that most of the Organization's submissions focus on the usefulness of a key fob system for allowing residents to securely access the building and its amenities. However, the issue is not whether key fobs are an effective device for controlling access to a building. Rather, the issue is whether a reasonable person would find the Organization's purpose for collecting and using personal information from the key fob system to be appropriate in the circumstances.

[236] For the reasons given above, I conclude the Organization's submission and evidence falls short of establishing that its purposes for collecting and using personal information from the key fob system is appropriate, as required under s. 11 of PIPA. The Organization did not establish that collecting and using personal information from its key fob system to track and monitor every strata resident's arrivals, departures and their movements and activities throughout the strata complex is appropriate for security purposes.

---

[157] Cover letter to Organization's submission dated August 20, 2018.
[158] Organization's submission dated August 20, 2018 at p. 3.

Using the key fob system for bylaw enforcement

[237] The complainant alleges the Organization is using the collected information in the key fob database to investigate and enforce a bylaw that prohibits short-term accommodation. The complainant says strata council members at the 2016 annual general meeting were congratulating themselves for their proactive surveillance policies for rule/by-law enforcement.[159] The complainant says the strata council shared that a staff member was proactively scanning the key fob logs for rule or by-law enforcement in real time, without an associated complaint.

[238] The complainant alleges that, despite not having a corresponding complaint, staff confronted a guest after seeing them with a suitcase on video surveillance and asked them personal questions based on the key fob database. He says when the guest did not know some of the details contained in the key fob database, in this instance the name of the unit owner's uncle, the staff then deactivated the key fob and the person was unable to access the property.

[239] The Organization denies that this incident took place as described by the complainant. It says the concierge became aware of a unit that was being advertised and used as a short-term accommodation rental by observing the movements of different people attending the suite and an online posting of the unit on a short-term accommodation rental website.[160] The Organization says the person with the suitcase admitted they were a vacation rental guest when the concierge engaged them in conversation and the guest left shortly afterwards.

[240] As noted previously, I am satisfied the Organization has a bylaw prohibiting short-term accommodation.[161] However, I am not satisfied the Organization is using personal information from the key fob database to question potential short-term accommodation guests in the way the complainant alleges. For instance, it is unclear me to who is the source of the information the complainant relies on as the basis for this allegation and how the complainant heard of it.

[241] The complainant's submission suggests he may have been told this story by a strata council member, but this is not clear and the description of this incident lacks any verifying details. I find there is simply not enough information or evidence to support the complainant's version of this incident. Therefore, without more, I am not persuaded that personal information collected by the key fob system was used to question and identify an alleged short-term accommodation guest.

---

[159] Complainant's submission dated May 27, 2020 at p. 2.
[160] Organization's submission dated June 9, 2020 at p. 2.
[161] The complainant provided a copy of one page from the strata's bylaws (page 7 of 30).

[242] The complainant also alleges the Organization is inappropriately using personal information collected from the key fob system to deny elevator access to fobs associated with units that violate the bylaw prohibiting short-term accommodation.[162] The complainant explains that this is done by using information in the key fob database to deactivate people's key fobs so they are unable to access the elevator and thus their strata unit.

[243] The Organization admits to using personal information from the key fob database to restrict elevator access to any unit in contravention of the bylaw prohibiting the use of strata units for short-term accommodation. The Organization says that, in 2020, the strata council did restrict elevator access to any unit that was being used for short-term accommodation purposes.[163] It says a number of buildings in its area were doing this. However, the Organization explains that after a couple of weeks, it decided that this was not a good idea for safety reasons and stopped doing it.

Is the Organization's use of personal information to restrict elevator access appropriate?

[244] The next step in the analysis is to determine whether using the personal information from the key fob database to implement the rule restricting elevator access was an appropriate purpose. The standard is an objective one and the question is whether a reasonable person would consider this purpose to be appropriate in the circumstances.

[245] The Organization did not provide any evidence to establish that using personal information from the key fob database to block elevator access as a means of enforcing its bylaw prohibiting short-term accommodation is appropriate. Instead, the Organization acknowledges that the new rule was not a good idea for safety reasons and so it rescinded the rule.

[246] Taking all of this into account, I conclude the Organization's use of personal information for this purpose was inappropriate and the Organization was in breach of PIPA.

Personal information collected and used for a fob inventory

[247] When residents are assigned a key fob, they are required to fill out a form identifying their unit number, telephone number, fob number, their name and their status as an owner, agent or tenant of the strata lot.[164] The Organization says that it collects this information so it can conduct fob audits. The Organization's audit consists of checking fob allocation from time to time to identify fobs that

[162] Complainant's submission dated May 27, 2020 at p. 2.
[163] Organization's submission dated June 9, 2020 at p. 2.
[164] Complainant's submissions dated September 19, 2018 and May 27, 2020.

need to be deactivated because they are missing or stolen. The Organization provided one example where a resident had nine key fobs registered to their unit, but could only account for seven key fobs. The Organization says fob audits are done for the security of the building and it is normal practice for a building of its age and type. It believes lost and stolen fobs are a huge security risk.

[248] The complainant does not believe lost fobs are a security risk and questions what evidence there is to support this claim. The complainant says it is unlikely that a lost key fob poses a security risk because the person would have to know certain information in order to use the fob, such as the strata building's address and the floor number that the key fob allows a person to access. The complainant believes that it is unlikely that this information would be known to a person who finds a lost fob since the fobs have no identifying information.

[249] The complainant also questions why the system cannot be anonymized. In response, the Organization says it would be difficult for it to conduct fob audits and disable lost or stolen fobs if it did not know which fob was assigned to which resident.

> *Is the collection and use of personal information for a key fob inventory appropriate in the circumstances?*

[250] I am satisfied that the Organization collected personal information about owners and residents to compile and maintain a fob inventory. I find this collected information is not sensitive. The Organization is required to obtain most of this information as part of its responsibilities in managing the strata corporation. For instance, s. 35 of the *Strata Property Act* requires the strata corporation to prepare and retain a list of owners and tenants, including their name and strata lot address or mailing address. Further, the amount and type of information collected seems appropriate to create an accurate fob inventory, including the collection of a telephone number. I find it reasonable to conclude that the telephone number would allow the Organization to easily contact the individual if needed to collect the correct information or for follow-up questions.

[251] I also find collecting this type of personal information is a logical and effective way for the Organization to acquire the information it needs to conduct a fob audit for security purposes. The collected information would allow the Organization to identify the number of key fobs in use and determine whether any are missing. This compiled information would allow the Organization to deactivate any unaccounted key fobs, thus reducing the likelihood that a key fob would fall into the hands of an unauthorized individual.

[252] I note that the complainant does not believe a lost key fob is a security risk because there is no identifying information on the key fobs. I agree that there may be instances where a lost key fob does not pose a security risk. However,

I find it reasonable for the Organization to be proactive in reducing its security risks rather than hoping that a person who finds a lost key fob on the strata grounds or nearby will not realize that it gives access to the strata buildings.

[253] In terms of alternatives, the complainant suggests that an anonymized key fob system would be more appropriate. However, the Organization says it would be difficult for it to conduct fob audits and disable lost or stolen key fobs if it is unable to identify to whom the key fob belongs.

[254] I find the Organization's explanation is reasonable since an anonymized system would make it more challenging to identify which key fob is missing and to remotely deactivate that fob. It may be possible for the Organization to conduct a fob audit without knowing to whom each fob has been assigned. However, I find it appropriate for the Organization to choose a more practical and efficient way, considering the non-sensitive nature of the information and how effective it is for achieving the Organization's security purposes.

[255] Therefore, considering the above factors and the circumstances overall, I am satisfied that the Organization's collection of personal information for the purposes of a creating and maintaining a fob inventory is appropriate.

2) Does the purpose of the collection and use comply with either ss. 11(a) and 14(a) or ss. 11(b) and 14(c)?

[256] If the purpose is appropriate, then the next step in the ss. 11 and 14 analysis is to consider whether the purpose of the collection and use fulfills the purposes that the organization discloses under s. 10(1) or whether it is otherwise permitted under PIPA.

[257] The relevant sections under ss. 11 and 14 are the following:

> 11 Subject to this Act, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> > (a) fulfill the purposes that the organization discloses under section 10 (1), or
> >
> > (b) are otherwise permitted under this Act.
>
> 14 Subject to this Act, an organization may use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> > (a) fulfill the purposes that the organization discloses under section 10 (1),
> >
> > …or

(c) are otherwise permitted under this Act.

[258] I note that the provisions of ss. 11(a) and 11(b) and the provisions of ss. 14(a) and 14(c) are each separated by the disjunctive word "or". Therefore, if the purpose for the collection and use is found to be appropriate, then that purpose need only comply with either ss. 11(a) and 14(a) or with ss. 11(b) and 14(c) in order for the requirements under ss. 11 and 14 to be satisfied.

[259] After considering all of the Organization's stated purposes, I found only the Organization's collection and use of personal information for the following purposes to be appropriate:

- To enforce its bylaws regarding garbage disposal through the use of video surveillance.
- To prevent and investigate property damage in the parkade area through the use of video surveillance.
- To create and update a key fob inventory by requiring residents to fill out and submit a form.

[260] Therefore, it is only necessary to consider whether those specific purposes comply with either ss. 11(a) and 14(a) or with ss. 11(b) and 14(c).[165] I will consider below each of the three purposes to determine whether they fulfill the purposes that the Organization discloses under s. 10(1) or are otherwise permitted under PIPA.

To enforce garbage disposal bylaws

[261] I found the Organization's use of video surveillance to collect and use personal information for the purpose of enforcing its garbage disposal bylaws was appropriate in the circumstances. The question then is whether the Organization disclosed this purpose under s. 10(1). As previously discussed, I find the Organization provided notice under s. 10(1) by posting a sign by the entrance to the garbage and recycling room that informs owners, residents and visitors that 24 hour video surveillance is being used to prevent the improper dumping of garbage. Therefore, I conclude the Organization's collection and use of personal information for the purpose of preventing the improper dumping of garbage complies with ss. 11(a) and 14(a).

[165] In terms of use, s. 14 requires that the Organization's purpose for using the personal information also comply with either s. 14(a), (b) or (c). Section 14(b) is not relevant for the purposes of this inquiry so I have not considered it in my analysis.

To prevent and investigate property damage in the parkade area

[262] I found the Organization's use of video surveillance to collect and use personal information for the purpose of preventing and investigating property damage in the parkade area was appropriate in the circumstances. By providing a copy of Bylaw 44, I find the Organization provided notice to owners and residents, under s. 10(1), of this appropriate purpose. Bylaw 44 says the video files will be used by the Organization for surveillance and monitoring purposes only, including preventing, recording, investigating and obtaining evidence of any vandalism or damage caused by any person on the strata plan.

[263] I also found the Organization provided notice to visitors of this purpose in accordance with s. 10(1). The Organization established that there is a sign posted on one exterior door with a picture of a video camera that notifies visitors the building is under 24 hour surveillance for security purposes, along with a phone number to call. I also accept that there is similar signage posted in the areas under video surveillance, including the parkade area. As a result, I find that the Organization's collection and use of personal information for the purpose of preventing and investigating property damage in the parkade area complies with ss. 11(a) and 14(a).

To create and update a key fob inventory

[264] I found the Organization's collection and use of personal information for the purpose of creating and a conducting a key fob inventory was appropriate in the circumstances. I also found the Organization provided notice under s. 10(1) by information provided on the form that owners and residents were required to fill and further information provided by the strata council to residents about why the Organization was collecting the personal information and what it would be used for. As a result, I conclude the Organization's collection and use of personal information for the purpose of creating and updating a key fob inventory complies with ss. 11(a) and 14(a).

[265] To summarize, I find that the requirements under ss. 11 and 14 are satisfied for the three above-noted purposes since notice was given as required under ss. 11(a) and 14(a).

Conclusion on the Organization's collection and use under PIPA

[266] For the most part, I conclude the Organization's collection and use of personal information was not in compliance with PIPA, even though the Organization provided notification and obtained consent in accordance with PIPA for most of these purposes. With three exceptions, I find a reasonable person would consider the Organization's purposes for collecting and using personal information to be inappropriate in the circumstances under ss. 11 and 14.

[267] The three exceptions are the Organization's collection and use of personal information for the purposes of enforcing its bylaws regarding garbage disposal, to prevent and investigate property damage in the parkade area and to create and update a key fob inventory. I conclude a reasonable person would consider the collection and use of personal information for these purposes to be appropriate in the circumstances. I also find the Organization provided notification and obtained consent in accordance with PIPA for these purposes. As a result, the Organization's collection and use of personal information for these three purposes complies with PIPA.

CONCLUSION

[268] For the reasons given above, under ss. 52(3) and 52(4), I make the following order:

1. I confirm the Organization is in compliance with PIPA regarding its collection and use of personal information for the following purposes:

    a. to enforce its garbage disposal bylaws;

    b. to prevent and investigate property damage in the parkade area; and

    c. to create and update a key fob inventory.

2. Except for the purposes identified in item 1 above, I require the Organization to stop collecting and using personal information through its video surveillance system.

3. I require the Organization to stop collecting and using personal information through its key fob monitoring system.

4. I recommend the Organization provide owners and residents with a complete list of all the video camera locations.

5. I require the Organization to provide the OIPC's registrar of inquiries with information and evidence that proves it complied with the above requirements.

[269] I also conclude a reasonable person would not consider it appropriate for the Organization to use personal information from the key fob database to block elevator access as a means of enforcing its short term accommodation bylaw. Considering the Organization has stopped this practice, I find an order directing them to stop using the personal information in such a manner is not necessary.

[270] Section 53(1) of PIPA requires the Organization to comply with this order no later than August 12, 2021.

[271] Lastly, I want to emphasize that this order is not a blanket prohibition against the future use of electronic surveillance by the Organization.[166] As the Commissioner's delegate, my responsibility is to apply PIPA based on the evidence and argument actually before me in this inquiry. For the reasons given above, I found that the Organization's collection and use of personal information through its video surveillance system and its key fob monitoring system for some purposes was not in compliance with PIPA.

[272] However, an organization's use of electronic surveillance may comply with PIPA if there is sufficient evidence and circumstances that meet the test as outlined in this order. Electronic surveillance should only be implemented after a thoughtful assessment of the need for it, in light of evidence as to its effectiveness, including whether alternatives are likely to be effective and the privacy impacts of the surveillance. It is, therefore, open to the Organization to conduct a privacy impact assessment, in future, to help it decide whether a reasonable person would consider electronic surveillance to be appropriate in the circumstances prevailing at that time.[167]

June 29, 2021

ORIGINAL SIGNED BY

Lisa Siew, Adjudicator

OIPC File No.: P17-70250

[166] Order P09-02, 2009 CanLII 67292 (BC IPC) at para. 89, point 4.
[167] The OIPC has guidelines and a template on its website to assist organizations with conducting a privacy impact assessment.