ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER P2006-008

March 14, 2007

LINDSAY PARK SPORTS SOCIETY, registered as TALISMAN CENTRE (trade name), and operating as TALISMAN CENTRE FOR SPORT AND WELLNESS

Case File Number P0253

Office URL: http://www.oipc.ab.ca

Summary: A complaint was made against the Organization which operates the "Talisman Centre for Sport and Wellness". The Complainant stated that the Organization had placed overt security cameras in the Talisman Centre's men's locker rooms. The Complainant was concerned about a loss of privacy and that patrons of the Centre would be unable to change without being viewed by the cameras. The Organization stated that the security cameras were installed in 1997 in response to over 900 incidents of theft and property damage during the years 1994-97. The security cameras were installed after all other means to prevent criminal activity had failed. The cameras' field of vision was restricted to the lockers and had no zoom, panoramic or audio capabilities. The cameras were not actively monitored and a protocol was in place which restricted the viewing of images to instances where there was an incident or reported criminal activity with a case number assigned by the Calgary Police Service. Viewing of the images occurs only in the presence of two senior staff members or by one such member and a police constable. If images are not reviewed they are automatically overwritten in approximately 21 days. After installation of the cameras there was a sharp reduction in criminal activity. As of the date of the Organization's submission to the Commissioner only 19 images had ever been viewed. The Commissioner found that due to the history of theft, the attempt to use other measures prior to using security cameras as a last resort, and the fact that the

images recorded were only accessed in the event of a criminal incident, that the Organization's collection of personal information was for purposes that were reasonable, as required by section 11(1) of the *Personal Information Protection Act* ("PIPA"). However, the Organization's signage was not in compliance with section 13(1) of PIPA. The Commissioner ordered the Organization to change the signage.

Statutes Cited: AB: *Health Information Act*, R.S.A. 2000, c.H-5, *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 1(6), 2, 8(2), 11, 11(1), 11(2), 13(1), 34, 56(1)(a), 56(1)(b), 56(3).**CAN:** *Canadian Charter of Rights and Freedoms* [being Schedule B to the *Canada Act 1982* (U.K.) 1982 c.11], *Personal Information and Protection and Electronic Document Act* S.C. 2000, c.5, ss.7(1).

Authorities Cited: *Concise Oxford Dictionary*, 9th edition,(Clarendon Press: Oxford 1995); *Guide to Using Surveillance Cameras in Public Areas,* Access and Privacy Branch, Alberta Government Services, June 2004; *Guidelines of Using Video Surveillance Cameras in Public Places,* Privacy Commissioner of Ontario, October 2001; *Public Surveillance System Privacy Guidelines*, Privacy Commissioner of British Columbia, (OIPC Reference Document 00-02), July 21, 2000; *Law of Torts*, P.H. Osborne, 2nd edition (Toronto: Irwin Law Co. 2003); *Sullivan and Driedger on the Construction of Statutes*, 4th edition (Toronto: Butterworths Canada Ltd. 2002); *The Law of Evidence*, Sopinka, Lederman and Bryant, 2nd edition, (Toronto: Butterworths Canada Ltd. 1999).

Cases Cited: *Eastmond* v. *Canadian Pacific Railway* [2004] F.C.J. No.1043; *R.* v. *Edwards* [1996] 1 S.C.R. 128; *Re: Rizzo and Rizzo Shoes Ltd*. [1998] 1 S.C.R. 27; *R.* v. *Schwartz* [1988] 2 S.C.R. 443; *R.* v. *Sharpe* [2001] 1 S.C.R. 45; *R.* v. *Stone* [1999] 2 S.C.R. 290.

Orders Cited: AB: Order 97-004, 97-011, 2000-002, P2005-001.

Investigation Reports Cited: **AB:** P2005-IR-004, P2006-IR-005.

I. BACKGROUND

[para 1] The Organization operates the "Talisman Centre for Sport and Wellness" (the "Talisman Centre") serving the general public since 1983. The Talisman Centre is the second largest sports facility in North America. It is open to the public from 5:00 a.m. to 11:00 p.m., Monday to Friday, 6:00 a.m. to 10 p.m. Saturday and Holidays, and 7:00 a.m. to 10:00 p.m. Sundays, 364 days a year. The Talisman Centre employs approximately 250 people and served, by its own estimates, 1.4 million patrons in 2004 and 1.6 million patrons in 2005.

[para 2] The Complainant wrote to me, complaining that the Organization had security cameras in the men's locker room at the Talisman Centre. The Complainant was concerned about a loss of privacy and that patrons of the Centre would be unable to

change without being viewed by the cameras. Mediation was unsuccessful and the matter was set down for a written inquiry.

[para 3] Other than an initial letter of complaint, the Complainant did not provide a written submission for the inquiry. The fact that the Complainant did not provide a submission in itself led to the Organization's request that additional issues be addressed, such as the requirement to file a submission, and who bears the burden of proof. I agreed that these issues should be heard and subsequently allowed for further submissions to be made by both parties. The Organization provided me with a submission on these additional issues, while the Complainant, again, did not provide a submission.

II. RECORDS AT ISSUE

[para 4] There are no records at issue.

III. ISSUES

[para 5] I have included the matters set out in the Notice of Inquiry as well as three further matters which the Organization raised during the Inquiry. As the first three issues deal with my jurisdiction to conduct the inquiry, I will deal with them as preliminary issues. The nine issues in this inquiry are:

A. Is the Complainant required to file a submission in the Inquiry?

B. Does the Complainant's failure to file a submission amount to a withdrawal of the complaint?

C. Does the Complainant's failure to file a submission and/or meet a burden of proof require the Commissioner to terminate the inquiry?

D. Is the Organization a non-profit organization, as provided by section 56(1)(b)?

E. If the Organization is a non-profit organization, is the Organization collecting personal information in connection with a commercial activity carried out by the Organization, as provided by sections 56(1)(a) and 56(3) of PIPA?

F. Is the Organization collecting personal information for purposes that are reasonable, as required by section 11(1) of PIPA?

G. Is the Organization collecting personal information only to the extent that is reasonable for meeting the purposes for which the information is collected, as provided by section 11(2) of PIPA?

H. Before or at the time of collecting the personal information, has the Organization complied with the requirements for notification set out in section 13(1) of PIPA?

I. Has the Organization protected the personal information that it collected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction, as provided by section 34 of PIPA?

IV. PRELIMINARY ISSUES

A. Is the Complainant required to file a submission in the Inquiry?

[para 6] The Organization argues that the burden of proof in this inquiry lies with the Complainant as it is a generally accepted principle of law that, absent a statutory provision to the contrary, the burden of proof lies on the party making the complaint and not the party defending it.

[para 7] The Organization submits that the Complainant, as the party with the burden of proof in this inquiry, must adduce sufficient evidence to meet his evidentiary burden and present an argument to meet his legal burden, at least on a *prima facie* basis. As the process in the inquiry is to present the Commissioner with written submissions, the Complainant must meet these burdens through the filing of a written submission with evidentiary support. By not providing submissions, the Complainant has not met either his legal or evidentiary burden.

[para 8] In *R v. Stone* [1999] 2 S.C.R. 290, the Supreme Court of Canada cited Sopinka, Lederman and Bryant, *The Law of Evidence in Canada* which contrasted the evidential burden with the legal or persuasive burden as follows:

> The significance of the evidential burden arises when there is a question as to which party has the right or the obligation to begin adducing evidence. It also arises when there is a question as to whether sufficient evidence has been adduced to raise an issue for determination by the trier of fact. The legal burden of proof normally arises after the evidence has been completed and the question is whether the trier of fact has been persuaded with respect to the issue or case to the civil or criminal standard of proof. The legal burden, however, ordinarily arises after a party has first satisfied an evidential burden in relation to that fact or issue.

[para 9] The *Personal Information Protection Act* ("PIPA") like the *Freedom of Information and Protection of Privacy Act* (the "FOIP Act") is silent with regard to where the burden of proof rests for an inquiry into a complaint about the collection, use and disclosure of personal information. In Order P2005-001, I adopted the approach previously taken in Order 97-004 with regard to the FOIP Act that addressed the burden of proof issue and applied the following criteria:

a) who raised the issue; and

b) who is in the best position to meet the burden of proof

[para 10] Relying on these criteria in Order P2005-001, I stated that a complainant has to have some knowledge of the basis of the complaint and it made sense to me that the initial burden of proof can, in most instances, be said to rest with the complainant. An organization then has the burden to show that it has authority under the Act to collect, use and disclose the personal information.

[para 11] This initial burden is what has been termed the "evidential burden". As I have said, it will be up to a complainant to adduce some evidence that personal information has been collected, used or disclosed. A complainant must also adduce some evidence about the manner in which the collection, use or disclosure has been or is occurring, in order to raise the issue of whether the collection, use or disclosure is in compliance with the Act.

[para 12] One of the purposes of the Act is to ensure that organizations collect, use or disclose information for purposes that are reasonable. Accordingly, the threshold for the evidential burden will be low, to allow a matter about an organization's compliance with the Act to be decided in an inquiry. It therefore follows that the Act does not require that a complainant meet a stringent burden of proof as may be required in a court of law, so as to allow a matter about an organization's compliance with the Act to be decided in an inquiry.

[para 13] In most cases the nature of the complaint will dictate the degree of evidence necessary to establish the basis of the complaint. For example, in Order P2005-001 the Complainant was concerned about disclosure of personal information to websites, employees of the Organization and to third parties. To sustain such a complaint a certain level of specificity in evidence was needed to identify the personal information disclosed and to whom. Usually, this is accomplished by a complainant making a submission detailing the nature of the complaint with supporting evidence.

[para 14] In this instance, the Complainant submitted a complaint letter. A complaint letter may be before me in an inquiry, as it is one of the documents that establishes my authority to conduct the inquiry. The complaint letter, although brief, does set out sufficient detail of the complaint. The Complainant has stated that there are cameras in the Organization's premises located in the men's changing room, a place where, arguably, a person has an expectation of privacy.

[para 15] As stated in Sopinka, Lederman and Bryant, *The Law of Evidence in Canada* at page 59, the incidence of the evidential burden means that a party has the obligation to adduce evidence or point to evidence on the record to raise an issue. The Complainant has adduced uncontested evidence that there are security cameras in the men's locker rooms. The fact there are cameras in such a location presents a unique circumstance which in itself is sufficient to raise issues as to the reasonableness of collection of personal information and the other attendant issues raised in this inquiry.

[para 16] As stated in by the Supreme Court of Canada in *R. v. Schwartz* [1988] 2 S.C.R. 443 at paragraph 38:

> The party with an evidential burden is not required to convince the trier of fact of anything, only to point out evidence which suggests that certain facts existed.

[para 17] As the Complainant has raised the initial issue as to the reasonableness of the Organization's collection of personal information, it will be the Organization who will be best placed to demonstrate the reasonableness of such collection and the other issues raised in this inquiry. The Complainant has raised a *prima facie* case. The Organization is far better placed than the Complainant to meet the burden of proof with regard to the issues touching its commercial activities, the authority and reasonableness of its collection of personal information and the security and notification arrangements undertaken.

[para 18] Finally, with regard to the Complainant meeting the legal burden in this inquiry, I refer to Sopinka, Lederman and Bryant, *The Law of Evidence in Canada* at p. 58:

> In civil proceedings, the legal burden does not play a part in the decision-making process if the trier of fact can come to a determinate conclusion on the evidence. If, however, the evidence leaves the trier of fact in a state of uncertainty, the legal burden is applied to determine the outcome. In *Robins v. National Trust Co*. the Privy Council explained the operation of the legal burden in civil cases as follows:
>
> > But onus as a determining factor of the whole case can only arise if the tribunal finds the evidence pro and con so evenly balanced that it can come to no sure conclusion. Then the onus will determine the matter. But if the tribunal, after hearing and weighing the evidence, comes to a determinate conclusion, the onus has nothing to do with it, and need not be further considered.

[para 19] I do not envision complainants having a legal burden under the Act. The Complainant's burden ends with having met the evidential burden, as discussed. The Organization then bears the evidential burden to demonstrate that its collection, use and disclosure of information is in accordance with the Act.

[para 20] I believe that the Organization is concerned that I am placing a "reverse onus" on it to prove a negative, that is, to prove that it did not breach the Act. On the contrary, the burden is on an organization to show that it has the authority under the provisions of the Act to collect, use or disclose personal information. This is the same burden of proof that is on a public body under the FOIP Act and a custodian under the *Health Information Act*.

[para 21] As will become apparent in this Order, I have concluded that there is sufficient evidence to determine the outcome of this inquiry without a reliance on the legal burden.

B. Does the Complainant's failure to file a submission amount to a withdrawal of the complaint?

[para 22] I have decided that the Complainant's complaint letter contained sufficient evidence to discharge the evidentiary burden. Furthermore, I find that a failure to file a submission does not amount to a withdrawal of the complaint. As discussed in Order 97-011, I agree that the onus will be on a complainant to withdraw his complaint and to inform me accordingly.

C. Does the Complainant's failure to file a submission and/or meet a burden of proof require the Commissioner to terminate the inquiry?

[para 23] My jurisdiction to conduct an inquiry and issue an Order is not dependent upon a complainant filing a submission and/or meeting a burden of proof. Section 50 of the Act provides that, if a matter is not settled pursuant to mediation, I may conduct an inquiry. Once an inquiry is commenced, section 52(1) of the Act requires that I dispose of the issues by making an order. Consequently, the only way to halt an inquiry and the order-making process would be if a complainant withdrew the complaint. In this instance, the Complainant has not made such a request.

[para 24] Further, section 50(3) of the Act states that the parties to an inquiry must be given an opportunity to make representations; it does not state that a person is required to make a submission. As the Complainant has not withdrawn from the inquiry and by his complaint letter discharged the evidentiary burden, there is no requirement to terminate this inquiry.

V. DISCUSSION OF INQUIRY ISSUES

D. Is the Organization a non-profit organization, as provided by section 56(1)(b) of PIPA?

[para 25] Section 56(1)(b) states:

> 56(1) In this section,
>
> (b) "non-profit organization" means an organization
>
> (i) that is incorporated under the *Societies Ac*t or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*, or
>
> (ii) that meets the criteria established under the regulations to qualify as a non-profit organization.

[para 26] The Organization has given affidavit evidence and attached as an exhibit a Certificate of Incorporation demonstrating that Lindsay Park Sports Society has been

incorporated under the *Societies Act*. It accordingly meets the definition of a "non-profit organization" under section 56(1)(b) of PIPA.

E. If the Organization is a non-profit organization, is the Organization collecting personal information in connection with a commercial activity carried out by the Organization, as provided by section 56(1)(a) and 56(3) of PIPA?

[para 27] At the outset, "personal information" is defined in subsection 1(k) of the Act as "information about an identifiable individual". This inquiry deals with the issue of security cameras. When a security camera records, it is capturing information. If an individual in the frame can be identified, then the captured image is "information about an identifiable individual". The information recorded by the camera therefore constitutes information about identifiable individuals and falls within the broad category of personal information under the Act.

[para 28] The Organization says that the images recorded by the security cameras are only viewed by the Organization if there is an incident or reported criminal activity. At the date when submissions were received in this inquiry, the Organization reported that only 19 images had been viewed. The Organization, therefore, submits that prior to determining whether or not it collects personal information in connection with a commercial activity, it must first be determined when the collection of personal information takes place in the context of the images captured by the security cameras.

[para 29] Specifically, the Organization relies on *Eastmond v. Canadian Pacific Railway* [2004] F.C.J. No.1043 which concluded that the "collection" of personal information only takes place when a recorded image is viewed. The Organization argues that if collection takes place at that point, the reason for its collection is for the purposes of a police investigation and not for any commercial purpose. Accordingly, PIPA does not apply to such activities, or alternatively, if there is a commercial activity, it is limited to the 19 images which were viewed by the Organization and not to the images that were recorded but never viewed.

[para 30] Having reviewed the *Eastmond* decision, I do not think it can be determinative in deciding when a "collection" takes place under PIPA. Firstly, it cannot be ascertained what arguments were made in this regard. Lemieux J. only states that he accepts Canadian Pacific's argument, although the decision itself does not state what that argument actually is. Secondly, at paragraph 189 Lemieux J. states that the definition of when a "collection" took place is in the context of section 7(1) (collection without knowledge or consent) of the *Personal Information and Electronic Documents Act ("PIPEDA").* Section 56(3) of PIPA has an entirely different purpose and construction than section 7(1) of *PIPEDA.*

[para 31] Section 56(3) of *PIPA* reads:

> 56(3) This Act applies to a non-profit organization in the case of personal information that is collected, used or disclosed by the non-profit organization in connection with any commercial activity carried out by a non-profit organization.

[para 32] In interpreting section 56(3), I must bear in mind the principles of legislative interpretation. The Supreme Court of Canada in *R. v. Sharpe* [2001] 1 S.C.R. 45 has cited with approval *Re: Rizzo and Rizzo Shoes Ltd*. [1998] 1 S.C.R. 27, wherein that court declared its preference for the "modern principle" of statutory interpretation. The principle is set out in *Sullivan and Driedger on the Construction of Statutes* at page 1 as:

> Today there is only one principle or approach, namely, the words of an Act are to be read in their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.

[para 33] I therefore must interpret section 56(3) in light of the "modern principle" of statutory interpretation.

[para 34] Reading the words of section 56(3) in their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, I cannot come to the conclusion that "collection" only takes place when stored images are actually viewed. "Collection" is defined by the *Concise Oxford Dictionary* as "1. the act or process of collecting or being collected. 2. a group of things collected together (e.g. works of art, literary items or specimens), esp. systematically." In the context of security cameras, the cameras systematically collect images, while any examination or review of those images is secondary to the act of collection.

[para 35] Such an interpretation is consistent with Order 2000-002 which, although in the context of the FOIP Act, defined "collection" as having obtained personal information in the first instance.

[para 36] To state that personal information is "collected" only when images are viewed also fails to consider the terms "used" and "disclosed" that are found in section 56(3) and "access" found in section 34. The *Concise Oxford Dictionary* defines "use": "1. cause to act or serve for a purpose; bring into service; avail oneself of…2.treat (a person) in a specified manner." "Disclose" is defined as: "1. make known; reveal (disclosed the truth) 2.remove the cover from; expose to view." While, "access" has been defined as: "a way of approaching or reaching or entering…2. the right or opportunity to reach or use."

[para 37] Given the ordinary dictionary meaning of those words, I find that in this instance, personal information is "collected" when images are recorded on the Organization's videotapes or hard drive of its computer.

[para 38] This interpretation is also in keeping with the scheme of the Act. Section 3 states the two purposes of the Act are to recognize the need of organizations to collect, use or disclose personal information for purposes that are reasonable and the right of an individual to have his personal information protected. It is also presumed that the provisions of legislation are meant to work together, both logically and coherently, as parts of a functioning whole. However, if I accepted *Eastmond*'s definition it would undercut section 11 of the Act that states an organization may only collect personal information for purposes that are reasonable. Instead, organizations would be able to amass huge numbers of videotapes for any purpose and be held to account only if they subsequently viewed the personal information collected. The reasons for collection would only have to become apparent at the time of the viewing not at the time the personal information was collected. The logistics of determining when "viewing" and hence "collection" took place would be formidable. I do not believe that the Legislature intended to limit the meaning of "collected" to "review" in these circumstances.

[para 39] Having dealt with the definition of "collected", I now turn to the purpose for which those images were collected. Since I have determined that personal information was "collected" at the time when the images were recorded, the personal information was not collected for a police investigation since none was instituted at that time.

[para 40] Section 56(1)(a) reads:

> 56(1) In this section,
>
> (a) "commercial activity" means
>
> (i) any transaction, act or conduct, or
>
> (ii) any regular course of conduct,
>
> that is of a commercial character and, without restricting the generality of the foregoing, includes the following:
>
> (iii) the selling, bartering or leasing of membership lists or of donor or other fund-raising lists;
>
> (iv) the operation of a private school or an early childhood services program as defined in the *School Act*;
>
> (v) the operation of a private college as defined in the *Post-secondary Learning Act*;

[para 41] The evidence presented by the Organization itself demonstrates that patrons can only use the facilities upon paying a daily or monthly or annual admission fee. The affidavit evidence of the Organization demonstrates that the collection of personal information by the security cameras was due to concerns that criminal activity was affecting the security of its premises which in turn had an effect on its commercial

activities. The affidavit evidence of the Manager of Operations from 1988-1999 at paragraph 7 stated that:

> The Talisman Centre believed that the increasing number of thefts and property damage in the men's locker room was a serious and legitimate issue that needed to be addressed because of a lost sense of security among patrons, harm to the reputation of the Talisman Centre and concern about the economic consequences of lost business as a result of patron's [sic] concerns about the security of their belongings.

[para 42] The General Manager and Chief Operating Manager from 1993-2000 deposed at paragraph 4 of his affidavit:

> …the considerable number of thefts and property damage in the men's locker room was a serious and legitimate issue that needed to be addressed, as it affected the reputation of the facility, caused distress to customers, undermined the sense of security of both staff and patrons, led to lost business from patrons who chose to end their memberships and potential patrons who elected not to become members because of security issues and imposed extra costs upon the Talisman Centre to repair the damage.

[para 43] The reason for the collection of personal information, therefore, was to improve security which in turn would impact on the Organization's mandate and commercial viability. I, therefore, conclude that personal information was collected in connection with a commercial activity in accordance with section 56(1)(a) of the Act.

ISSUE F: Is the Organization collecting personal information for purposes that are reasonable, as required by section 11(1) of PIPA?

[para 44] Section 11 of PIPA states:

> 11 (1) An organization may collect personal information only for purposes that are reasonable.
>
> (2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the the purposes for which the information is collected.

[para 45] Section 2 of PIPA sets out the standard to determine what is reasonable. It reads:

> 2 Where in this Act anything or matter
>
> (a) is described, characterized or referred to as reasonable or unreasonable, or
>
> (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,
>
> the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt

> with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

[para 46] An analysis of section 11(1) requires me to determine the purpose for which the Organization is collecting personal information and whether that purpose is reasonable.

[para 47] The Organization has presented evidence and submits that it has collected personal information through the use of security cameras for the purpose of detecting and deterring criminal activities in the men's locker room. I accept that this is the purpose for which the Organization collected personal information.

[para 48] When I review the collection of personal information to determine if it was collected for reasonable purposes, I am applying an objective standard. I am not allowed to substitute whether I would collect the information if I were the Organization. That is, I do not have to personally agree with the collection and I could still find it to be reasonable.

[para 49] The notion of reasonableness is central to the Act. Organizations are generally called upon to collect, use and disclose personal information in a reasonable manner. It is not an easy concept to apply. Osborne, *The Law of Torts* says this (Substitute the word "organization" for the word "person") at chapter 2, page 2:

> The reasonable person is not therefore any single person. It is not appropriate for a judge or juror, for example, to evaluate the defendant's conduct on the basis of what she would have done in similar circumstances. Neither is the average person the reasonable person…In truth, the reasonable person is an abstract legal construct, used to set appropriate standards of conduct in society. That standard is determined by taking into account both the practical realities of what ordinary people do and what judges believe they ought to do. It is not, however, a standard of perfection. The reasonable person may make errors of judgment for which there is no liability.

[para 50] So the question is: Is it reasonable for the Organization, being the operator of a fitness facility, faced with these issues, to collect personal information by installing surveillance cameras in the men's locker room in this manner?

[para 51] Tests have been developed to apply this standard.

[para 52] In determining the reasonableness of that purpose, the Organization has proposed that I use the four-part test set out in *Eastmond* as an appropriate analytical base. This test was originally developed by the former Privacy Commissioner of Canada in that matter to determine the reasonableness of the use of security cameras in an employment context. On the judicial review of that matter, both parties agreed to apply the test, although Lemeiux J. remarked that the factors set out in it may not necessarily be relevant in other contexts.

[para 53] As I have already discussed, *Eastmond* proceeds under the logic that there would be no collection since there was no viewing. But this causes problems with respect

to security: a great deal of information is “machine collected”, never viewed by human eyes, yet the Legislature must have intended that those who possess the information be responsible for it whether or not they have “seen” it.

[para 54] Rather than limiting the definition of “collection”, as *Eastmond* would suggest, I think it is preferable to have regard to the continuum of “collection-use-disclosure”. Even if large amounts of personal information can be collected, use and disclosure are still limited. In the case of “machine collected” information which consists of a large volume of material that has been collected, the principle that use and disclosure may occur only for purposes that are reasonable functions as a limitation to ensure that personal information is used or disclosed in accordance with the Act. Suppose a machine collected the information and nothing else was ever done with it. *Eastmond* would suggest “no collection, no use, no disclosure.” The continuum would suggest “collection, no use, no disclosure”. The collector is still responsible for any use, all disclosures and security.

[para 55] Of course, from a privacy point of view, it is preferable to not collect it in the first place: subsequent use, disclosure and security issues then never arise. You avoid issues of function creep, the temptation to put the information to other uses because you do have it. Collection is significant because it is the first step down that road: avoid the collection and you avoid all the other dangers. But if the information can legitimately be collected, the next consideration is that it not be used or that it be used in the most limited way. And, if it can legitimately be collected, and legitimately be used, the final consideration is that it not be disclosed or be disclosed to the least number of recipients.

[para 56] I prefer to use the criteria set out in my Office’s *Investigation Report P2005-IR-004* to determine the reasonableness of the collection of personal information by video surveillance. Although that Report dealt with security cameras in the employment context, it was specifically guided by the actual wording of PIPA, its legislative purposes and the rules of statutory interpretation. The criteria were:

1) Does a legitimate issue exist to be addressed through the collection of personal information?

2) Is the collection of personal information likely to be effective in addressing the legitimate issue?

3) Is the collection of personal information carried out in a reasonable manner?

[para 57] I therefore shall use these factors to determine whether the collection of personal information by the use of security cameras for detecting and deterring of criminal activities is a reasonable purpose under section 11(1).

1. Does a legitimate issue exist to be addressed through the collection of personal information?

[para 58] The men's locker room at the Talisman Centre is approximately 1,334.5 square feet of developed space and contains 302 individual lockers. There are seven security cameras located in plain view on the ceiling of the men's locker room.

[para 59] The Manager of Operations for the Organization from 1988 to 1999 has deposed that from the period 1994 to 1997 a high number of thefts from the men's locker room were reported. He gave the following breakdown of theft and property damage incidents occurring in the men's locker room:

1) For 1994 to 1995 there were approximately 200 incidents;

2) For 1995 to 1996 there were approximately 300 incidents;

3) For 1996 to 1997 there were approximately 400 incidents.

[para 60] An affidavit from the General Manager of the Organization from 1993 to 2005 gave similar evidence and also deposed that many of the thefts appeared to be the work of an organized criminal enterprise.

[para 61] The General Manager further deposed at paragraph 6 of his affidavit that:

> In or about 1995, I directed to be undertaken the following steps in an attempt to resolve the problem of locker room thefts, including:
>
> a) Researching and installing stronger, more resistant metal clasps for the lockers;
> b) Reading several internal reports, and reports from other sports facilities concerning locker room thefts;
> c) Discussing the locker room thefts with similar facilities with a view towards finding out if these facilities faced similar problems and what preventative means were used;
> d) Approaching the City of Calgary, Insurance and Calgary Police Services for input and guidance;
> e) Reviewing literature on technologies available;
> f) Contacting the Talisman Centre's insurer for suggestions; and
> g) Convening several conference calls and meetings among Talisman Centre managers to discuss the locker room thefts and potential solutions.

[para 62] From these inquiries and research the Organization attempted numerous security measures prior to the installation of security cameras, which included:

1) Making structural modifications to the lockers to make them more secure;

2) Installing alarm systems in lockers;

3) Introducing “dummy” lockers to spray dye on persons attempting to remove materials from these lockers;

4) Posting notices warning patrons to be alert to suspicious behaviour;

5) Providing wallet lockers outside the men’s locker room for the storage of valuables;

6) Scheduling staff to walk through the men’s locker area on a regular basis;

7) Scheduling custodians to remain in the men’s locker room during peak periods, and

8) Hiring professional security guards to patrol the men’s locker room.

[para 63] The Organization’s employees deposed that these measures met with limited success and the problems of theft and property damage to the men’s locker rooms remained. The Operations Manager deposed that modifications to lockers while successful in the short-term soon became ineffective once thieves started using larger pry-bars.

[para 64] The General Manager deposed that:

1) The alarm system did not reduce theft as thieves were able to make an exit prior to a response;

2) Dummy lockers spraying dye while effective in eliminating theft by employees, was ineffective as regarding the public at large who could exit without detection;

3) The notices were ineffective as patrons still preferred to bring their own locks which thieves were able to circumvent using different types of tools;

4) Wallet lockers were ineffective as patrons chose not to use them;

5) The locker room was open from 15 to 18 hours a day. Patrols by security staff did not diminish the incidence of theft as they

> occurred outside the time of the patrols and the physical structure of the locker room prevented staff from being able to visually cover the entire locker room at any one time.

[para 65] The Organization's evidence is that it was only after these measures failed that a proposal regarding the installation of security cameras in the men's locker room was approved by Organization's Board of Directors in or around October 1997.

[para 66] I find given the level of theft and property damage at the Talisman Centre that the detection and deterrence of criminal activity became a legitimate issue for the Organization and that its unsuccessful attempt to use alternate measures made this an issue which was proper to address through the collection of personal information.

2. Is the collection of personal information likely to be effective in addressing the legitimate issue?

[para 67] I have found that the detection and deterrence of criminal activity was a legitimate issue for the Organization to address. As to the effectiveness of the collection of personal information by the use of security cameras, the Manager of Operations deposed that after the installation of security cameras, there were approximately 10 thefts in the men's locker room during the period of 1997-1998 and 1998-1999. These incidents were described by him as "crimes of convenience" and none were the result of forcible entry which prior to the installation of security cameras had been the most predominant type of theft. I conclude from this evidence that the security cameras have been an effective means of addressing this issue.

[para 68] At this point I must emphasize in the strongest possible way a significant difference between surveillance cameras in a locker room and surveillance cameras in public places like a street. The objective of the cameras in the locker room is not to reduce crime across society: it is in fact to push the criminals out of that locker room. The thieves may well go somewhere else, such as a locker room where there aren't cameras. Similarly, if the objective of cameras on a public street is to make that street safer, that may be achieved by pushing the criminals out. But it may be achieved at the expense of other streets where the criminals disperse to. If the objective of the surveillance cameras on a public street is to make society safer, the research, which I will not go into here, indicates that they will not succeed. For this reason any surveillance scheme must be carefully thought out.

3. Is the collection of personal information carried out in a reasonable manner?

[para 69] The next step is to determine whether the collection of personal information by security cameras is carried out in a reasonable manner. *Investigation Report P2005-IR-004* considered the following circumstances relevant in arriving at such a determination: the type of surveillance, the accessibility of recorded images and whether there was any reasonable alternative.

[para 70] I think the most intrusive type of surveillance would be real-time monitoring via camera; i.e.,- a bank of monitors at a security desk, plus recording. People are being watched and recorded. Next would be monitoring by security staff or locker room attendants. People are being watched but not recorded. Next would be, as in this instance, being recorded but not watched.

[para 71] The Organization submits that consideration must be given as to whether an individual would have a reasonable expectation of privacy when using the men's locker rooms. In terms of a discussion on the type of surveillance used, I would assume that if no one has an expectation of privacy, the issue as to the type of surveillance and the attendant issue of intrusiveness would not arise.

[para 72] The Organization argues that as the facilities are open to the public and at any given time approximately 300 males could be in the process of changing and showering, there would not be a significant expectation of privacy when using the locker room.

[para 73] The Supreme Court of Canada in *R. v. Edwards* [1996] 1 S.C.R. 128 addressed the issue of expectation of privacy, albeit as it relates to the *Canadian Charter of Rights and Freedoms*, in the context of unreasonable search and seizure. It stated that a reasonable expectation of privacy is to be determined on the basis "of the totality of the circumstances." While I recognize that this case is not relevant to PIPA, it nevertheless makes sense to me that I should consider the totality of the circumstances when considering an expectation of privacy in deciding whether collection of personal information is carried out in a reasonable manner.

[para 74] In entering a locker room an individual's expectation of privacy is to some extent formed by an individual's own expectations and the characteristics of that facility. The affidavit of the current Operations Administration Director demonstrates the degree of the privacy present in the men's locker room. At the entrance there are 18 inch by 18 inch permanent signs reading "Video Surveillance Cameras on Site". There are smaller signs prohibiting the use of cell phones, presumably as a precaution against unauthorized photography.

[para 75] In the locker room there are seven security cameras located in plain view on the ceiling throughout the locker room. The design of the locker room itself obstructs any direct view from the entrance of changing areas. The entire changing area cannot be viewed from one vantage point. The shower and washroom areas do not have security cameras. Recognizing the inherently private nature of changing and showering and the limitations of privacy in a large, busy locker room, the Organization offers in the alternative Executive lockers with private showers and family change rooms with cubicles.

[para 76] I cannot agree with the Organization's submission that there would not be some expectation of privacy when using a locker room. I believe that an individual would consider that the very nature of changing affords some expectation of privacy; at the very

least there is an expectation that other patrons using the locker room are there for similar purposes and are not mere bystanders. Concerning the use of security cameras, I believe that there is a further expectation of privacy that the images recorded will only be used for the limited purpose for which the cameras were installed. This limited purpose is stated in the "Talisman Centre Privacy Policy" as:

> …These cameras are in high risk areas. When in use, surveillance cameras are there for the protection of employees and third parties, and to protect against theft, vandalism and damage to goods and property. Video tape recording images are routinely destroyed and not shared with third parties unless there is suspicion of crime, in which case they may be turned over to the police or other appropriated government agency or authority.

[para 77] During this inquiry I accepted an affidavit deposed by the current Operations Administration Director on an *in camera* basis. I accepted this affidavit on an *in camera* basis as the evidence deposed therein pertains to the integrity of the Organization's security system, which if made public would undermine the security measures taken. This affidavit contains photographs that show each camera's field of vision. In examining these photographs, the information deposed and the floor plan of the locker room, I am satisfied that the cameras have been placed where the majority of thefts and property damage take place and accordingly, the area was chosen because that was where the thefts and property damage occurred.

[para 78] I further refer to the former Manager of Operations' affidavit that states that the installed cameras are without any audio, zoom or panoramic capabilities. Furthermore, and significantly, the cameras are not used to monitor the activities in the locker room in real time. No one is able to watch people getting changed. There is no bank of monitors to be viewed. The cameras record only to a secure location. The cameras are motion-activated and capture a person's image only when they are within the field of vision of the camera.

[para 79] Although this may be a less intrusive type of surveillance, in any situation, we become uncomfortable or worse when someone watches us. Someone stares at you across a room or in a coffee shop. If the stare is broken by a smile or wave, it becomes less unnerving perhaps, because the subject of the stare now has a clue to the watcher's motive. Similarly, knowing that you are being followed by someone is unnerving and intrusive. In certain cases, we call this "stalking". If the follower's motives are known, i.e., a parent following a young child, a bodyguard, a uniformed police officer on a dark street, we might feel good about being followed.

[para 80] The issue of being naked adds another dimension to these sensitivities. When one goes to the doctor, the doctor always leaves the examining room when the patient is getting changed. The doctor is still going to see the patient naked, but will not see the patient changing. There is something about being watched, under the gaze of another human, while taking our clothes off or putting them on, which is very intrusive.

[para 81] I am aware that some individuals may be of the opinion that even being recorded without being watched is too intrusive a type of surveillance to place in a

changing room. However, I refer to *Obsorne's* definition of the "reasonable person" wherein I must look to the practical realities of the situation before me. As has been previously discussed, in this instance, a legitimate issue existed to be addressed through the collection of personal information. The cameras are in plain view and of limited capability. There are signs to inform patrons of the existence of the cameras and alternate changing rooms are available. The collection of personal information has been effective in addressing this legitimate issue. I, therefore, find that that the type of surveillance undertaken by the Organization results in a privacy intrusion that is no greater than is necessary.

[para 82] I now turn to the second circumstance considered in *P2005-0IR-004*: that of the accessibility of the recorded images.

[para 83] I have reviewed the Organization's protocol for the access and retention of recorded images, which was included as an exhibit to the *in camera* affidavit. This protocol demonstrates that there is a controlled access area separated by various locked doors from the general access areas. The images are stored on a stand-alone computer unconnected to any internal or external network. Access to the computer and images are both password protected. Only four senior male employees of the Organization have authority to view the tape and viewing is never allowed unless an investigation had been initiated and assigned a police number and two staff members or one staff member and one police constable are present. If images are not viewed, they are automatically overwritten in approximately 21 days. Having reviewed this evidence I have concluded that the accessibility and storage of the recorded images is properly protected.

[para 84] This leaves me to consider whether there was any reasonable alternative to the surveillance undertaken by the Organization. I have already discussed this issue during the examination of whether a legitimate issue existed to be addressed through the collection of personal information. There is sufficient evidence to conclude that alternate measures were undertaken and it was only after the failure of these measures that a decision was taken to install the security cameras. Accordingly, there are no other reasonable alternatives.

[para 85] Finally, I find it relevant to have considered the extent to which there has been an actual loss of privacy. In this instance, the actual loss is minimal given that the cameras are not actively monitored and the protocol sets out the procedures for the reviewing and retention of images.

Conclusion

[para 86] As has been deposed, the Organization was faced with years of theft and property damage. In response it had used various measures, all unsuccessful, prior to using security cameras. The security cameras successfully met the problem. The cameras are not surreptitious. Warning signs are displayed. The cameras have a limited field of vision and capabilities. The recorded images are accessed only in the event of an incident and in the presence of male senior managers and police.

[para 87] In applying the criteria to the evidence before me, given the unique circumstances particular to this matter, I conclude that a reasonable person would consider the Organization's collection of personal information by the use of security cameras for the purpose of detecting and deterring criminal activities to be appropriate in the circumstances. In making this finding I must state that had the Organization considered active monitoring or viewing images beyond the strictly limited purposes stated in this case, it would have been highly unlikely to have met the reasonableness test.

[para 88] I would further add that the Organization should make efforts to review and evaluate its video surveillance program on an ongoing basis, to ascertain in light of future circumstances whether video surveillance remains justifiable under the Act.

[para 89] I must add one final comment. During this inquiry I made reference to the the general principles published in the *Public Surveillance System Privacy Guidelines*, (OIPC Reference Document 00-01) July 21, 2000 issued by the Privacy Commissioner of British Columbia, the *Guidelines of Using Video Surveillance Cameras in Public Places*, October 2001 issued by the Information and Privacy Commissioner of Ontario and the *Guide to Using Surveillance Cameras in Public Areas*, June 2004, produced by the Access and Privacy Branch of Alberta Government Services (the "guidelines").

[para 90] All the guidelines referenced have a degree of consensus. I have considered the principles most relevant to the situation at hand and for the sake of brevity have placed them in three general headings which encompass the planning and installation of security cameras and the retention of images recorded. These principles are contained in an Addendum to this Order. However, I emphasize that the principles do not assist in determining what is a reasonable collection of personal information in a particular fact situation, such as this one.

G. Is the Organization collecting personal information only to the extent that is reasonable, for meeting the purposes for which the information is collected, as provided by section 11(2) of PIPA?

[para 91] Given the location, field of vision and limited capabilities of the cameras combined with the protocol for viewing images, I find that the Organization is collecting information only to the extent that is reasonable for meeting the purposes for which the information is collected.

H. Before or at the time of collecting the personal information, has the Organization complied with the requirements for notification set out in section 13(1) of PIPA?

[para 92] The relevant portions of section 13 read:

> 13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally

> (a) as to the purposes for which the information is collected, and
>
> (b) of the name of a person who is able to answer on behalf of the organization the individual's questions about the collection.
>
> (4) Subsection (1) does not apply to the collection of personal information that is carried out pursuant to section 8(2).

[para 93] The Organization has reproduced in its affidavits the notices set out at the Talisman Centre and throughout the men's locker room. All of the signs state that there is video surveillance on site. No purpose for the collection of personal information is provided. The signs inside the men's locker room further state that if a patron has any questions to contact the Operations Department.

[para 94] The Organization submits that a reasonable person upon seeing the prominent signage notifying them of the existence of security cameras and viewing the cameras themselves, would understand that their personal information may be collected for the purposes of detecting and deterring criminal activity.

[para 95] However, the wording of section 13(1) is clear. An organization must notify an individual in writing or orally as to the purposes for which information is collected. There is no provision under this section that the purpose of collection can be inferred. Likewise, a notice must state the name of a person able to answer questions not as, is the current practice, the responsible department of the Organization.

[para 96] In the alternative, the Organization may avail itself of section 13(4) of PIPA wherein section 13(1) of the Act will not apply if section 8(2) is applicable. Section 8(2) reads:

> 8(2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an Organization for a particular purpose if
>
> (a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for the purpose, and
>
> (b) it is reasonable that a person would voluntarily provide that information.

[para 97] The Organization submits that an individual who chooses to enter the locker rooms after seeing the signage notifying him of the existence of cameras and observing the cameras has voluntarily provided his personal information as contemplated in subsection 8(2) of PIPA.

[para 98] However, deemed consent has to be for a particular purpose. It is difficult to conclude how an individual upon reading the wording of the signage and viewing the cameras, can sufficiently identify the purpose for which their personal information is

being collected. Had the Organization provided wording in its signage similar to that reflected in its privacy policy, it may have availed itself of section 8(2). However, given the signage as it now stands, the requirements of section 8(2) cannot be met in this instance. Accordingly, the Organization has not complied with the requirements set out in section 13(1) of the Act.

I. Has the Organization protected the personal information that it collected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction, as provided by section 34 of PIPA?

[para 99] *Investigation Report P2006-IR-005* examined the issue of making reasonable security arrangements in accordance with section 34. It stated that the Act requires an organization to guard against reasonably foreseeable risks. An organization must demonstrate that it implemented deliberate, prudent and functional measures that display consideration toward risk mitigation in order to be in compliance with the Act. In addition, the nature of the safeguards and measures undertaken will vary according to the sensitivity of the personal information collected.

[para 100] I have reviewed the protocol attached as an exhibit to the *in camera* affidavit. As has been mentioned, it provides for a controlled access area separated by various locks from general access areas. Given the sensitivity of the personal information collected images are stored on a stand-alone computer unconnected to any internal or external network. Only four senior male employees of the Organization have authority to view the images and viewing is never allowed unless an investigation has been initiated and assigned a police number and two staff members or one staff member and one police constable are present. All images, if not viewed, are overwritten in approximately 21 days.

[para 101] Given these safeguards, I find that the Organization has made reasonable arrangements against the risks enumerated in section 34.

VI. ORDER

[para 102] I make the following Order under section 52 of the Act.

[para 103] I find that the Complainant is not required to file a submission in this inquiry.

[para 104] I find that the Complainant's failure to file a submission does not amount to a withdrawal of the complaint.

[para 105] I find that the Complainant's failure to file a submission does not require me to terminate this inquiry.

[para 106] I find that the Organization is a non-profit organization as provided by section 56(1)(b) of the Act.

[para 107] I find that the Organization is collecting personal information in connection with a commercial activity carried out by the Organization, as provided by section 56(1)(a) and 56(3) of the Act.

[para 108] I find that the Organization is collecting personal information for purposes that are reasonable, as required by section 11(1) of the Act.

[para 109] I find that the Organization is collecting personal information only to the extent that is reasonable for meeting the purposes for which the information is collected, as provided by section 11(2) of the Act.

[para 110] I find that the Organization did not comply with the notification requirements set out in section 13(1) of the Act.

[para 111] I order the Organization to replace its current signage with signs that explain the purpose for the collection of personal information and the circumstances in which that personal information will be disclosed. Additionally, the signs will identify the names of staff who, on behalf of the Organization, can be contacted to answer questions regarding the collection of personal information. I order the Organization to comply with this requirement within 50 days and to provide me with a photograph of the new signage.

[para 112] I find that the Organization has protected the personal information it has collected by making reasonable security arrangements as provided by section 34 of the Act.

Frank Work, Q.C.
Information and Privacy Commissioner

Addendum to Order P2006-008

I refer to the general principles published in the *Public Surveillance System Privacy Guidelines*, (OIPC Reference Document 00-01) July 21, 2000 issued by the Privacy Commissioner of British Columbia, the *Guidelines of Using Video Surveillance Cameras in Public Places*, October 2001 issued by the Information and Privacy Commissioner of Ontario and the *Guide to Using Surveillance Cameras in Public Areas*, June 2004, produced by the Access and Privacy Branch of Alberta Government Services (the "guidelines").

All the guidelines referenced a degree of consensus. I have considered the principles most relevant to the situation at hand and for the sake of brevity have placed them in three general headings which encompass the planning and installation of security cameras and the retention of the images recorded. However, I emphasize that the principles do not assist in determining what is a reasonable collection of personal information in a particular fact situation, such as this one.

Planning of a surveillance system

1) Use of a surveillance system must be as a last resort and only where conventional means are substantially less effective;

2) The implementation should be on the basis of a verifiable specific problem;

3) There should be consultations with relevant stakeholders;

4) A Privacy Impact Assessment (PIA) should be completed to assess the effects that the proposed security cameras may have on privacy and the ways in which any adverse effects can be mitigated;

5) Areas chosen for surveillance should be those where surveillance is a necessary and viable deterrent;

6) The system shall be designed and operated so that the privacy intrusion it creates is no greater than absolutely necessary to achieve the system's goals;

7) There should be public notification, using clearly written signs with the address or telephone number of a contact person, prominently displayed at the perimeter of the surveillance areas.

Surveillance Records: Access and Retention

8) All tapes and records should be locked in a control access area with access only by authorized personnel;

9) There should be a policy on retention.

Cameras in Change Rooms/Locker Rooms

10) Only where there is a law enforcement issue. Not to monitor behaviour;

11) Should not be monitored in real-time. Too many opportunities for surreptitious viewing;

12) Should record and store only. View only in the event of a complaint, and then in the presence of police and senior staff;

13) Access extremely limited: senior staff. Must have log on and audit trail so it can be verified who has viewed;

14) Recordings must be secured;

15) No "online" access whatsoever;

16) Should not be kept. Record over within at reasonable time;

17) Never in lavatory areas. No matter what;

18) Cameras must be visible and notice provided;

19) If physically possible, change areas should be outside the scope of cameras.