Appendix A

Fieldwork Report on Video Surveillance and Signage in the Greater Toronto Area

An appendix to the 'Smart' Private Eyes in Public Places? report

Prepared for	Office of the Privacy Commissioner of Canada
Prepared by	Andrew Clement, Joseph Ferenbok, Roxanna Dehghan, Laura Kaminker & Simeon Kanev
	Information Policy Research Program, Faculty of Information, University of Toronto
Corresponding Author	andrew.clement@utoronto.ca
Date	23 July 2011

Table of Contents

Report on Fieldwork

1. Introduction

Video surveillance of the public by private sector organizations is now commonplace in Canada. Our actions are watched and recorded in the supermarket, the gym, in restaurants, even as we simply stroll on a sidewalk. As private-sector organizations capture our images, and gather identifiable information such as our gender, ethnicity, age group and other personal characteristics, they are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA).

The Office of the Privacy Commissioner of Canada (OPC) (2008) has determined that both video recordings and real-time video surveillance without recording constitute the collection of personally identifiable information; thus, the rights of request and access set forth in PIPEDA apply. PIPEDA also specifies that the public must be notified of the collection of personally identifiable information. In the case of video surveillance and video recording in publicly accessible private spaces, notification takes the form of signage informing the public of the use of such video. The signage should indicate how video surveillance is being used, how personally identifiable information will be stored or used, and individuals' rights regarding that use. Yet, to anyone familiar with PIPEDA and the guidelines from both federal and provincial privacy authorities regarding video surveillance in the private sector (OPCC, OIPCA, OIPCBC, 2008), compliance with PIPEDA, at least in the notification requirements, appears nearly nonexistent. To investigate further the video surveillance practices of private sector firms, and in particular their compliance with PIPEDA, the Private Eye research project was undertaken in 2010 with the financial support of a grant from the OPC's Contributions Program.

This report on the fieldwork aspects of the Private Eyes project will present the goals of the research, the methodologies employed, the principal findings, and the researchers' conclusions based on the data collected. The fieldwork was divided into three distinct phases. For Phases I and II, findings and analysis will be presented relating to the presence of video surveillance cameras, the presence of notification of surveillance (*i.e.*, signage), signage compliance with PIPEDA requirements, responses to researchers' interviews about companies' surveillance practices and policies, and responses to researchers' requests to access their personal information collected by video surveillance. Because Phase I and Phase II employed distinct samples and methodologies, some findings are presented separately for each phase. The analysis of signage compliance with PIPEDA requirements are presented in the aggregate for Phase I and Phase II fieldwork. Examples will be supported by representative photographic and other materials. The third phase of the fieldwork was conducted with a different methodology and purpose, and will be discussed separately.

2. Goals

The widespread use of video surveillance in the Greater Toronto Area (GTA) and the apparent lack of compliance with PIPEDA requirements were the starting points for the

fieldwork in this project. Under the supervision of University of Toronto professor Andrew Clement, researchers sought to document the use of video surveillance and to test such surveillance for relative compliance or non-compliance with PIPEDA requirements. Among the research questions asked were:

1. How extensive is video surveillance in the private sector in the GTA?

2. Are private-sector video surveillance operators aware of PIPEDA? Are they compliant with PIPEDA requirements?

3. What notification do video surveillance operators provide, both publicly and on request, about their use of such surveillance?

4. What can a individual expect in terms of the collection of their personally identifiable information? If an individual attempts to exercise her rights under PIPEDA, will her right to request and access that information be respected?

2.1 Relevant Legislation

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal, and in Province of Ontario, the principal legislation governing the use of video surveillance in the private sector. Private-sector organizations must comply with several PIPEDA principles when engaging in the collection, use, disclosure, retention, and destruction of personally identifiable information. Part 1, Section 2 of PIPEDA (2011) indicates that a

> record includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things (p. 3).

Thus the use of video surveillance, when it captures images of individually identifiable persons, is considered to be the collection of personal information, and as such, PIPEDA requirements apply. The following are excerpts from PIPEDA that directly apply to the collection of personal information through the use of video surveillance.

> Principle 1, Accountability
>
> 4.1.2
>
> The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request. (p. 34)

According to this section of Principle 1, Accountability, an organization must identify an individual to whom questions or concerns regarding privacy can be directed. The

Accountability principle includes the requirement to develop information explaining the organization's policies and procedures with respect to privacy, and with respect to handling inquiries and complaints.

> Principle 2, Identifying Purposes
>
> 4.2
>
> The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. (p. 34)

An organization must clearly state why and for what purpose it collects personal information, and must do so before the collection of that information. In the case of video surveillance, this would be best accomplished through signage notifying the public of the use of such surveillance. In order to comply with Principle 2, Identifying Purposes, the sign must be visible before the individual enters the surveilled area.

> Principle 3, Consent
>
> 4.3.2
>
> Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. (p. 36)

Under the Consent Principle, organizations employing video surveillance must announce to prospective surveillance subjects that they do so. As with the Identifying Purposes Principle, in the case of video surveillance, this requires signage that is informative and accessible to those entering the surveilled space.

> Principle 5, Limiting use, disclosure, and retention
>
> 4.5
>
> Personal information shall be retained only as long as necessary for the fulfillment of those purposes. (p. 38)
>
> 4.5.2
>
> Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. (p. 38)

Under Principle 5, personal information must not be retained indefinitely, but only until it has served the purpose for which it has been collected. Minimum and maximum retention periods should be specified and communicated.

> Principle 8, Openness
>
> 4.8.1
>
> Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. (pp. 39-40)
>
> 4.8.2
>
> The information made available shall include:
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
> (b) the means of gaining access to personal information held by the organization;
> (c) a description of the type of personal information held by the organization, including a general account of its use;
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> (e) what personal information is made available to related organizations (*e.g.*, subsidiaries). (p. 40)

The Openness Principles requires organizations engaging in video surveillance to develop policies regarding privacy and the collection of personal information, and to make those policies available to anyone who requests them.

> Principle 9, Individual Access
>
> 4.9
>
> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information
>
> 4.9.4
>
> An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. (pp. 40-1).

Principle 9, Individual Access grants individuals whose personal information has been collected access to that information, and requires organizations collecting that information to comply with this right.

The repeated use of the word “shall” in the above Principles is significant, as it signals legally enforceable requirements. Only Sec. 4.5.2 uses the weaker language of “should”.

This study sought to test the use of video surveillance in the private sector in the GTA with compliance with all of the above PIPEDA principles.

3. Methodology

We approached the fieldwork in three distinct phases. The first phase targeted the largest, most prominent firms in the private sectors which had most direct contact with the public. These in effect are the industry leaders in terms of video surveillance. The second phase targeted two of the largest shopping malls in the GTA – the Eaton Centre (TEC) and Square One in Mississauga, both very popular with consumers. The third phase targeted cameras that visibly surveilled public areas, notably public sidewalks. In all three phase we focused on the visible presence of surveillance cameras and any accompanying signage. Phases I and II also probed other aspects of the installations as well as organizational responses to individual queries about their video surveillance operations.

3.1 Phase I Fieldwork – Industry leaders

3.1.1 Sample, Phase I

Companies were selected for the Phase I sample according to four criteria: that PIPEDA requirements apply to their industry, that they have a point-of-contact with consumers, that they are likely to use video surveillance at that point-of-contact and that they are relatively prominent. Within these criteria, the Phase I sample was drawn in large part from the private-sector organizations listed in “2010 Top 1,000 Canadian Companies,” published by the *Globe and Mail Report on Business* (Globe & Mail, 2010). Thirty of the 45 organizations (66%) included in the Phase I sample are among the top 1,000 Canadian companies. Additional organizations in the Phase I sample were selected for their high commercial visibility in the GTA. These stores are all familiar names in the commercial landscape of Ontario and the GTA. Within the Phase I sample, there are representatives of several different industries that have a consumer-point-of-contact, such as retail stores, food service, and banks. Within the retail sector, industries are further divided by type. In each category, specific locations meeting the specified criteria were further selected because of their proximity to the researcher’s home in Mississauga, Ontario. In all, the Phase I sample comprises 45 organizations.

As some of the largest actors in their respective industries, the policies of these organizations are implemented in many different locations, and therefore, affect great numbers of consumers. In addition, industry leaders often set trends, as the policies

they adopt become industry standards. In this sense, researchers believe that the Phase I sample is representative of many large corporations doing business in the GTA.

Table 1 shows the list of organizations and site locations used in the Phase I sample.

Table 1: Phase I Sample by Industry	
Sector	**Organization**
Banking	
	Bank of Montreal
	Canadian Imperial Bank of Commerce (CIBC)
	Royal Bank of Canada (RBC)
	The Bank of Nova Scotia (Scotia Bank)
	TD Canada Trust
Department Stores	
	Canadian Tire
	Costco
	Sears
	Zellers
Food	
	McDonald's
	Pizza Hut
	Pizza Pizza
	Starbucks
	Swiss Chalet
	Tim Horton's
Hotel	
	Marriott Hotel
Retail	
Building Supplies	
	Home Depot, The
	Rona
Electronics	
	Bell Mobile Store
	Best Buy

Table 1: Phase I Sample by Industry	
Sector	**Organization**
	Best Buy Mobile
	Future Shop
	Source, The
Entertainment	
	Blockbuster
	Chapters
	Famous Players Cinema
Clothing	
	Le Chateau
	H&M
	Mark's Work Wearhouse
	Reitman's
	Winners
Home Furnishings	
	Home Outfitters
	Leon's
Supermarkets	
	Highland Farms
	Loblaws
	Metro
	Price Chopper
Specialty	
	Beer Store, The
	Black's
	Shoppers Drug Mart
	Sport Chek
	Staples
	West 49

The Phase I sample was selected, in part, because of the presence of video surveillance in the organization's consumer point-of-contact. Thus, this phase of the research was not intended to evaluate the prevalence of video surveillance. Phase I

focused on the presence of notification of video surveillance and compliance of that notification with PIPEDA requirements, especially with respect to PIPEDA Principles 2, Identifying Purposes, and Principle 3, Consent. Phase I also sought to discover the treatment an individual might encounter while attempting to exercise her rights under PIPEDA, especially with respect to Principle 8, Openness and Principle 9, Individual Access.

3.1.2 Methods, Phase I

After a pilot study involving the full research team, in July 2010 researcher Simeon Kanev began approaching the organizations selected for the Phase I sample. Most of the 45 companies were contacted in August 2010 and the fieldwork was completed by October of that year.

For each site in the sample, the researcher recorded some general data (see below for details about the recording methods): name and location of organization, date and time of visit, type of organization (bank, supermarket, specialty store, etc.). The researcher photographed the storefront, any visible video cameras and any visible signage relating to the use of video surveillance. (All relevant fieldwork photographs are available on the Flickr photo-sharing website, in a group called “Canadian Surveillance Camera (aka CCTV) Signage”. See notes for URL.)

Signage was photographed both close-up, to show the exact text of the sign, as well as from a distance, to show the size and placement of the sign in context of the storefront. These details speak to several inter-related research goals. What information, if any, do consumers receive about the use of video surveillance? Are consumers notified of the presence of video surveillance before they enter a surveilled space, that is, do consumers have a choice whether or not their images are captured on video? Are consumers notified of the company’s privacy policies?

The researcher noted the number of cameras visible from the organization’s entrance, and whether or not, given the cameras’ location and apparent angle of view, a camera was likely to capture images of people who were not necessarily entering the store. The researchers find these instances particularly problematic with respect to privacy rights, as even a broad conception of security or loss-prevention justification cannot be said to apply to passersby. This data above is noted on the top portion of the Site Visit Protocol form. A sample of this form used in the Phase I fieldwork is attached as Appendix A, Fig. 1.

After the exterior of the site was assessed and documented, the field researcher entered the retail space, approached a staff member, and asked to speak to a manager or other responsible employee. If such a person was available, the researcher asked them a series of semi-structured questions regarding the company’s use of video surveillance, its policies relating to the use of video images, and the manager’s awareness of PIPEDA requirements. Responses were noted on the bottom portion of the Site Visit Protocol form. After a brief interview, the researcher presented the store manager with a Request for Personal Information form, requesting to obtain the video

footage captured during the researcher's visit. A sample of this form used in the Phase I fieldwork is attached as Appendix A, Fig 2.

The Request for Personal Information contained the name and address of the organization, a detailed description of the appearance of field researcher (recorded in advance of the site visit), the date of the visit, and the exact time of the visit, usually within a period of five minutes. The personal appearance description and narrow time frame are intended to assist the organization in identifying the exact video footage being requested. The researcher's name and contact information (address, telephone number and e-mail address) were also provided on the form.

Additionally, the form references relevant excerpts from PIPEDA, including the above-mentioned Openness Principle, the requirement that personal information requests be complied with within 30 days, and the obligation of an organization to assist an individual preparing such a request. (For more detail, see the "Relevant Legislation" section of this report.)

3.1.3 Follow-up, Phase I

As part of the Phase I fieldwork, the researcher continued to contact organizations with which he submitted a Personal Information Request. The researcher called and e-mailed the organizations to remind them of their obligation under PIPEDA section 8(3) (2011) to respond within the specified 30-day period. If a response was not forthcoming within 30 days, the researcher attempted to contact the organization's accountable person, such as a chief privacy officer or privacy coordinator. If this reminder did not receive a response, the researcher would wait an additional 30 days, then send a second reminder. No further reminders were sent.

3.2 Phase II Fieldwork – Major Shopping Malls

3.2.1 Sample, Phase II

The Phase II sample was drawn from two of the largest and most popular shopping centres in the GTA, the Toronto Eaton Centre (TEC) in downtown Toronto, and the Square One Shopping Centre (Sq1) in Mississauga, Ontario. According to the City of Toronto, TEC attracts one million visitors each week (City of Toronto, 2008); Cadillac Fairview Corporation Limited, which manages the TEC property, says it has a "total trade area of 3.6 million people" (Cadillac Fairview Corporation Limited [Cadillac]). Sq1 is the largest shopping centre in the province of Ontario (Oxford Properties [Oxford]**)** and the second largest indoor mall in Canada (Directory of Major Malls). Both TEC and Sq1 are official landmarks and promoted by their respective cities as tourism destinations; both receive millions of visitors each week.

Researchers intended to sample both shopping centres in their entirety. In the case of TEC, this was accomplished – all private sector organizations with publicly accessible spaces in TEC are included in the Phase II sample. While assessing Sq1, researchers were prevented from completing their fieldwork by the shopping centre's security forces, who claimed the research violated their policies and disrupted commerce. Detailed

discussion and analysis of this impediment to research, and its significance to the issues raised in this study, are found below in the section 4.6, “Shopping centre security response to research”. In all, the Phase II sample comprises 101 locations in Sq1 and 158 locations in TEC, a total of 258 locations. This also includes the common areas of both shopping centres. The Sq1 sample includes only the main mall, and not the numerous free-standing buildings that make up the entire shopping complex.

Phase II research tested the prevalence of video surveillance in the private sector, and (as in Phase I), the presence of notification of video surveillance and compliance of that notification with PIPEDA requirements, especially with respect to PIPEDA Principles 2, Identifying Purposes, and Principle 3, Consent. Phase II also tested the treatment individuals can expect to encounter while attempting to exercise their rights under PIPEDA Principles 8, Openness and 9, Individual Access.

3.2.2 Methods, Phase II

Phase II fieldwork was principally conducted by Roxanna Dehghan, a student at University of Toronto Mississauga, and secondarily by Laura Kaminker, a graduate student at the University of Toronto’s Faculty of Information. The methods employed by researchers in Phase II fieldwork were similar to those used in Phase I fieldwork. The most significant difference between the methodology of the two phases was the manner in which researchers identified themselves. In Phase I, researcher Kanev did not immediately identify himself as a researcher or disclose information about the research project, but did so if asked more specifically about the purpose of the visit. Kanev sought to re-create the experience a private citizen – a civilian, so to speak – might encounter when attempting to exercise his or her statutory right to access personal information collected by a private organization. In Phase II, researchers Dehghan and Kaminker immediately identified themselves as participants in a University of Toronto study funded by the Office of the Privacy Commissioner. Although such identification appears to have assisted Phase II researchers in gaining the attention of store managers, it made little difference in the outcome of their requests for personal information, nor did it assist when shopping centre management took an adversarial approach to the research project, as will be discussed below.

The Phase II research was conducted as follows. Researchers first assessed the storefront while standing outside the store (either in the mall, on the sidewalk or in the parking lot, depending on location), looking for the presence of both video surveillance and signage notifying the public of such surveillance. Researchers photographed the storefront, any signage, and any visible cameras. Signage was photographed both close-up to show the text of the sign and from a distance to illustrate how the sign appears to the public in context. The significance of these distinctions is discussed further in section 4.1, “Presence of video surveillance”, below. As in Phase I, researchers noted whether or not cameras on a site’s exterior were likely to capture images of individuals who were not necessarily entering the store. Researchers filled out the top portion of the Site Visit Protocol form. A sample of the form used in the Phase II fieldwork is attached as Appendix A, Fig. 3.

Researchers then entered the store location, identified themselves to a store employee as part of a research project being conducted by the University of Toronto, funded by the Office of Privacy Commissioner of Canada, studying video surveillance in the private sector, and asked to speak to a manager or other responsible employee. While waiting to speak to an appropriate employee, researchers looked for cameras and signage in the store, noted the presence of same on the Site Visit Protocol form, and, when possible, photographed cameras and signs.

If a manager was available and willing to be interviewed, researchers asked the questions indicated on bottom portion of the Site Visit Protocol form. Frequently, the employee would say that she was not authorized to answer questions, and direct researchers to a corporate office. In those cases, researchers collected the relevant contact information. The researchers asked permission to leave a Request for Personal Information form, briefly explaining that the form is a request to access video images of herself that were captured by the store's video surveillance system. Researchers would also show the relevant sections of PIPEDA on the reverse of form. An example of this form used in the Phase II fieldwork is attached as Appendix A, Fig 4. In Phase II, no follow-up was conducted regarding the Personal Information Requests. Photos were also posted to the Flickr group

3.3 Phase III Fieldwork – Open Street Surveillance

3.3.1 Sample, Phase III

In Phase III, researchers sought to sample, document and assess video surveillance and notification of such surveillance in public space in Toronto's downtown core. Downtown Toronto is a densely populated, urban area with a high concentration of both pedestrian and vehicular traffic. Previous to this study, researchers had observed the proliferation of video surveillance cameras throughout the downtown area, beyond those installed by the Toronto Police Service. As these cameras began to appear in the urban landscape, there was no public notice or discussion about who was operating these cameras or the purpose of the cameras. Researchers believe the public has not been informed about what type of surveillance is being used (whether live monitoring or recording), where and for how long images may be stored, who has access to these images, and similar questions concerning the collection of personal information. The Phase III sample was open-ended, drawn from heavily traveled areas in the downtown core. There was some overlap between the Phase II and Phase III samples. Some of these cameras featured in the "(Video) Eyes on the street" Jane's Walk of May 2011. (See surveillancerights.ca website)

3.3.2 Methods, Phase III

Phase III fieldwork was initially conducted by a team of student researchers led by Professor Clement, then continued by Roxanna Dehghan. Researchers walked through a chosen location in Toronto's downtown core looking for the presence of video surveillance cameras. When researchers noticed cameras, they would record the cameras' location and characteristics, and photograph the cameras. Researchers also

looked for any signage intended to notify the public of the use of these video surveillance cameras. Researchers would record the signs' characteristics, and photograph signs both close-up to the show the text of the sign, and from a distance to show the sign in context. Researchers recorded the characteristics of cameras and signage on a Camera Inventory Form. A sample of the form used in the Phase III fieldwork is attached as Appendix A, Fig. 5. The most significant difference between the methods employed in Phase III and those used in Phases I and II was that Phase III fieldwork did not involve interviews with employees or requests for personal information.

4. Findings

4.1 Presence of video surveillance

The Phase I sample was selected, in part, because of the likelihood of video surveillance in the publicly accessible spaces of the selected industries. Thus the presence of video surveillance cameras in the Phase I sample, as expected, was high, but we were surprised that 100% of the sample had some form of video surveillance.

In Phase II, video surveillance cameras were observed in 98 of the 258 locations (38%). In two locations, store employees told researchers that the cameras were dummies and did not work; the cameras' presence was meant to act as a deterrent to theft. In one location, researchers did not see cameras but were told that non-visible cameras were in place. In one additional location, researchers suspected the use of cameras hidden behind mirrors. Fig. 1 represents the presence of video surveillance cameras observed in the Phase II sample.

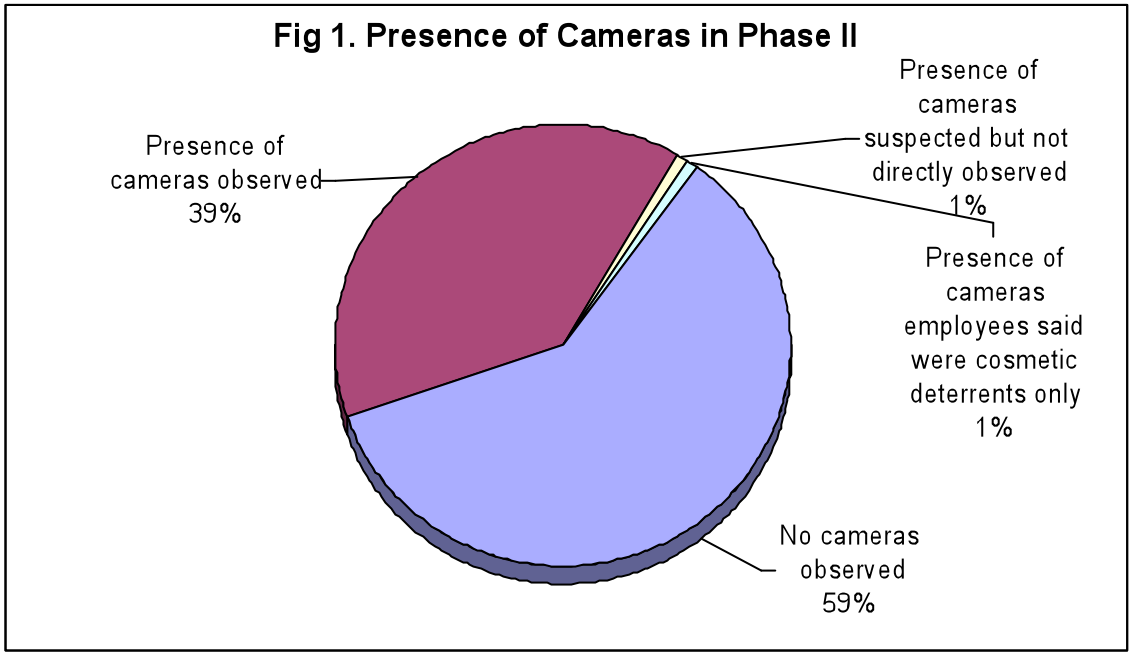
Of the 101 locations where video cameras were observed (this includes the two locations were employees told researchers the cameras were fake), 32 locations (32%) had video cameras on the exterior of the storefront. Of those 32 locations, researchers judged that in 23 locations (71%), cameras were likely to capture images of individuals not on the property of the surveillance operator; in an additional five locations, it was possible that the surveillance cameras were capturing such images. Researchers believe this type of surveillance is especially problematic, as there is no rational justification for an organization to use video surveillance on individuals simply walking in publicly accessible space near their storefront.

Numerous cameras were observed in the common areas of both TEC and Sq1. In TEC, researchers counted 21 cameras in the interior, and 15 cameras on the exterior, plus 12 cameras for which the operator was unknown or ambiguous. Almost all the exterior TEC cameras could potentially capture images of people not entering the TEC. In Sq1, researchers counted 45 cameras in interior common space. As noted above, this sample included only the main Square One mall, and not the numerous nearby free-standing buildings that make up the entire Square One complex.

While video surveillance cameras were not observed in approximately 60% of the Phase II sample, where video surveillance was observed, it was pervasive and nearly ubiquitous within the stores. In Sears, for example, one of the large anchors of TEC,

researchers counted 90 cameras, plus 12 additional cameras of ambiguous ownership that may belong to Sears. Within the TEC and Sq1 common areas, video surveillance is almost total; it is reasonable for a consumer to expect to be under surveillance constantly in either of these locations for their entire time within each mall. This will be discussed in more detail later in this report.

As Phase III employed an open-ended sample, the presence of video surveillance in this sample cannot be expressed as a percentage of locations sampled. It is quite



reasonable to say that researchers found the use of video surveillance in Toronto's downtown core to be pervasive and commonplace. In many instances, multiple cameras facing the public sidewalk were observed at one location. It was often unclear who was operating these cameras.

4.1.1 Presence of notification of video surveillance, Phase I

The rapid expansion of video surveillance in Canada can be seen everywhere, but signage that indicates the presence of such surveillance is not nearly as apparent. It seems that signage meant to "provid[e] surveillance subjects with meaningful information" about video surveillance practices is usually lacking (Clement & Ferenbok, 2011). Official guidelines on what information a sign must convey to surveilled subjects is already in place. The OPC, jointly with the Information and Privacy Commissioners of Alberta and British Columbia (2008), as well as the Office of the Information and Privacy Commissioner of Ontario (IPC) (2007), have issued guidelines for the use of video surveillance in the private sector. The requirement for signage is important because, as Lippert (2009b) shows, the sign lets individuals know not only about the presence of video surveillance, but the purpose for using it, as well contact information for potential

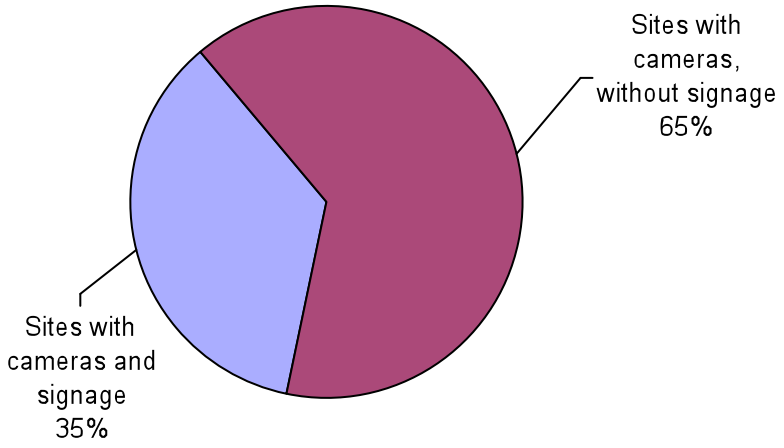
questions. However, as Clement and Ferenbok (2011) observe, the explicit notification requirements are found in guidelines that are meant to assist companies "with the deployment of their video surveillance systems and are not binding or enforceable" (p. 5). That is, the notification requirements enable private-sector video surveillance, but do little to protect consumers' privacy rights.

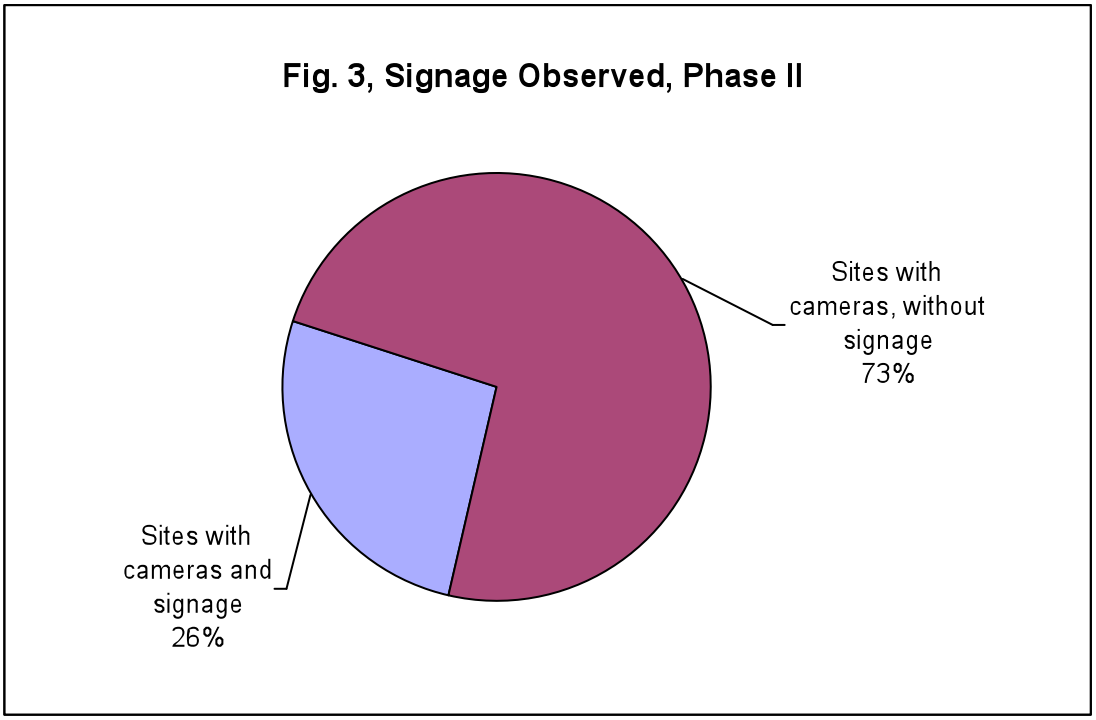
Fieldwork data clearly illustrates both the lack of signage generally and the lack of PIPEDA-compliant notification among private sector organizations with a consumer point-of-contact. As shown in Fig. 2 below, of the 45 locations sampled in Phase I, all of which used video surveillance, only 16 locations (35%) gave any public notification that video cameras were in use.

4.1.2 Presence of notification of video surveillance, Phase II

As shown in Fig 3 below, of the 99 locations sampled in Phase II where video surveillance was identified (this excludes the two locations where cameras were observed, but employees told researchers they were fake, and no video surveillance was in use), only 26 locations (26%) gave any public notification that cameras were in use.

Fig. 2, Signage Observed, Phase I





The high percentage of video surveillance in use without any corresponding notification – 65% in Phase I, 73% in Phase II – clearly violates PIPEDA Principle 2, Identifying Purposes:

> The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected (p. 34).

If video surveillance is in use without any form of signage or notification, then, clearly, the organization is collecting personal information without identifying the purpose for which it is being used either at or before the time of such collection.

The use of video surveillance without the presence of signage also violates PIPEDA Principle 3, Consent, which states:

> Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. (p. 39)

Finally, the use of video surveillance without corresponding notification also violates PIPEDA Principle 8, the Openness Principle. The Openness Principle requires that

organizations collecting private information, which includes personally identifiable images "...shall be open about their policies and practices with respect to the management of personal information" (pp. 39-40).

4.1.3 Presence of notification of video surveillance, Phase III

In the Phase III sample, signage notifying the public that video surveillance was in use was present in less than half (46%) observed instances of video surveillance. Moreover, that 46% is a generous figure that includes all signs, including signs that are barely visible and/or non-informative. For example, on the entrance to the TEC, in white lettering on a glass background, at the top of a large glass door, well above eye level, is a sign reading, "As part our management services, Cadillac Fairview uses closed circuit television at this property" (Appendix B, Fig. 1). The sign would not generally be visible to anyone who was not specifically searching for such signage, as our researchers were. Yet, at the same time, as many as 33 cameras were observed in TEC, at great distance from the entrance signage. Typically, when signage was observed during Phase III fieldwork, it was the generic "Warning: These Premises Protected By Video Surveillance," an example of which can be seen at Appendix B, Fig. 4.

4.2 Compliance of signage with PIPEDA requirements, all fieldwork

The issue of notification goes to more than the mere presence of signage. The size and placement of the signage, the information contained on the sign, and the public's ability to access and read the sign are all at issue. Under PIPEDA guidelines, organizations collecting private information must clearly state the purpose of such collection, and must do so *before* actually collecting it. In the case of video surveillance, this means the presence and purpose of video surveillance on an easily readable sign before individuals enter the surveilled space. This would allow the individual to decide whether they wish to enter the area, knowing that their personal information will be captured by the video surveillance equipment.

The specific features of signage, as well as the size and placement of the sign, relate to both Principle 2, Identifying Purposes, and Principle 3, Consent, quoted above, as well as PIPEDA Principle 8, the Openness Principle. The Openness Principle requires that organizations collecting private information, which includes personally identifiable images:

> ...shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort (pp. 39-40).

Principle 8 further states:

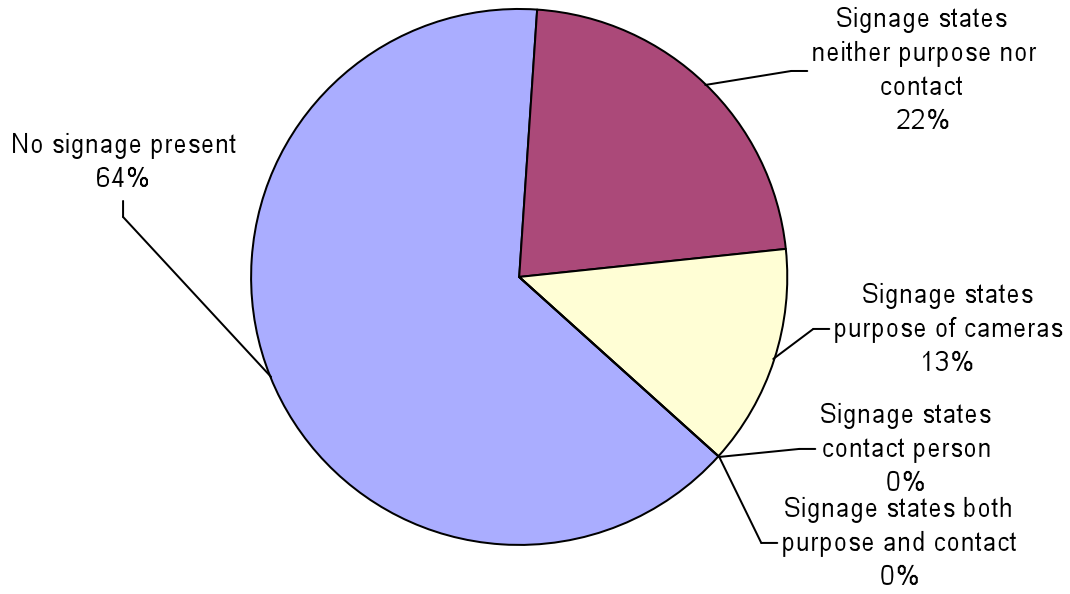
> The information made available shall include:
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and

> to whom complaints or inquiries can be forwarded;
> (b) the means of gaining access to personal information held by the organization;
> (c) a description of the type of personal information held by the organization, including a general account of its use;
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> (e) what personal information is made available to related organizations (e.g., subsidiaries)" (p. 40).

In both Phase I and Phase II samples, every sign observed was generally judged to be non-compliant with PIPEDA requirements. In Phase I, a small number of signs came a bit closer to PIPEDA standards. In Phase II, signs were grossly non-compliant, as analysis will show.

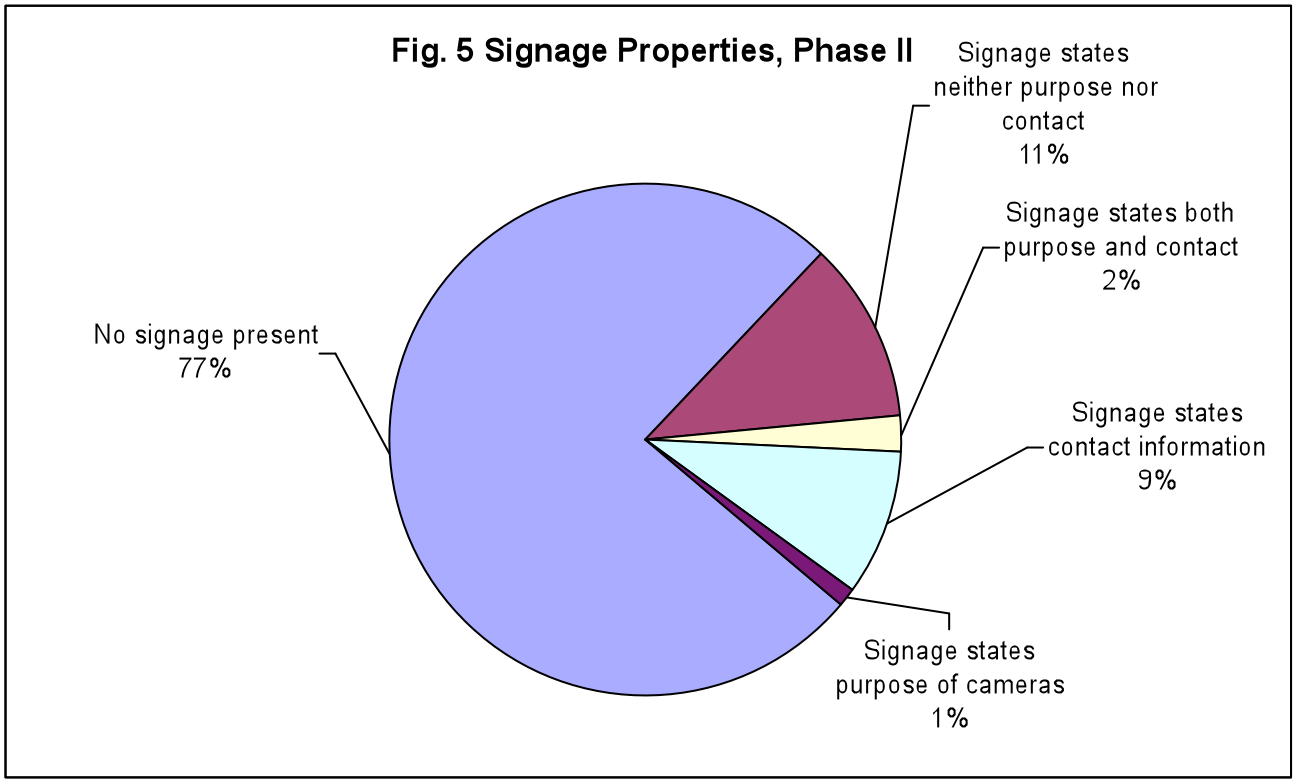
Fig. 4 illustrates several key properties of the signage observed on the premises of the organizations sampled in Phase I. Only 16 out of 45 (35%) organizations in the Phase I sample used any signage notifying the public of the presence of video surveillance. Of the 16 signs observed, most contained only a brief statement about the use of video surveillance, with variations on the theme of "Video Surveillance in Effect" or "Premises protected by CCTV surveillance system". When the text of the sign states a reason or purpose for the video surveillance, this is also framed in vague or generic terms, such as "for your protection" or "for the safety of our customers". These statements will be discussed in more detail in section 4.2.3, "Signage non-compliance: vagueness, ambiguity, misleading statements in text of sign".

Fig. 4 Signage Properties, Phase I



In Phase II, notification was observed even less frequently, with 77% of locations employing video surveillance cameras failing to display any notification of such surveillance. Among the 26 locations using any type of signage, full compliance with PIPEDA notification requirements was nonexistent. The observed signage was not only non-compliant with respect to the lack of appropriate information provided on the sign. In addition to the absence of information, every sign in the Phase II sample was also relatively inaccessible to anyone who could not be reasonably expected to search for signs, as our researchers were. Of the 26 signs observed, most were very small (Appendix B, Fig. 2), placed either far above (Appendix B, Fig. 1) or far below (Appendix B, Fig. 3) eye level, designed to blend in with the background (Appendix B, Figs. 1a, 1b) and otherwise barely visible (Appendix B, Figs. 3a, 3b). This is in sharp contrast with the many signs posted by these retail establishments to alert customers to other routine aspects of their operation, such as no-smoking, hours of operation, etc.

Fig. 5 Signage Properties, Phase II



The Excel sheet, *PIPEDA Compliance of Signage Observed in Phases I and II*, found in Appendix E documents the properties of each sign observed in both Phase I and Phase II fieldwork, detailing (non-)compliance with PIPEDA requirements. This PIPEDA compliance table also contains URLs for the Flickr Group where photographs of each sign can be seen, both in detail to show the sign's text and in context in its location. A more detailed analysis of signage non-compliance with PIPEDA requirements follows.

4.2.1 Signage non-compliance: placement and visibility of signs

One of the most frequent fieldwork observations was of signage that was barely visible. This lack of visibility was caused by the size of the sign relative to the storefront, the placement of the sign relative to the entrance, or both. The sign used by the store Pink (Appendix B, Fig. 3) illustrates this issue. The sign itself is about the size of a credit card, and has been placed on the extreme lower left corner of a very large plate glass display window, at about the height of an adult's ankle. The sign is not visible from the store entrance, so a customer entering the store does not see it. These issues of both size and placement issue were commonly observed by researchers, especially within the two shopping centres in Phase II.

The signs notifying the public of video surveillance systems in place in both TEC and Sq1 malls proper are particularly egregious violations in this category, and especially significant as they apply to the entire shopping centres. On the entrance to TEC, at the

very top of a set of large glass doors, in white lettering on a clear background, are the words, “As Part of Our Management Services Cadillac Fairview Uses Closed Circuit TV at This Property” (Appendix B, Figs. 1a, 1b). Only the keenest of observers who are already looking for signage would spot this. At the entrance to Sq1, on the very bottom of a large set of glass doors, there is a strip of pictograms, intended to serve as notice of the rules of the mall. For example, there is a graphic depiciting a dog with a line through it, symbolizing “no dogs allowed,” and a graphic depicting a shirt, symbolizing “shirts must be worn”. One such pictogram represents a video surveillance camera, with the words “CCTV security surveillance cameras in use” below the picture (Appendix B, Figs. 2a, 2b, 2c). Again, only an astute observer purposely searching for notification of video surveillance would see this. Indeed, both the TEC and Sq1 signs are so small and inaccessible that one can hardly call them notification. Contrast these signs with, for example, the large signs prominently displayed in TEC directing the public to public transit, elevators, washrooms and accessibility ramps (Appendix B, Fig. 5a, 5b, 5c). These signs are large, placed in central locations, using high contrast colours on a black background. One can see that when Cadillac Fairview, operator of TEC, wants to disseminate information to the public, they are able to do so. Based on this comparison, one can only conclude that Cadillac Fairview and Oxford Management, the operator of Sq1, do not want to inform the public about the use of video surveillance.

Cadillac Fairview Corporation and Oxford Properties, the management companies responsible for TEC and Sq1 respectively, are among Canada’s largest retail real estate management firms. According to its website, Cadillac Fairview is one of the largest commercial real estate managers in North America, with a real estate portfolio valued at more than $19 billion (Cadillac). Oxford Properties is a multinational real estate conglomerate. According to its website, Oxford Properties Canada “oversees one of the most valuable real estate portfolios in North America,” representing “more than 40 million square feet of office, retail, hotel, industrial, land and multi-residential assets in key markets across Canada” (Oxford). The practices of such large retail management companies affect significant numbers of Canadian consumers and are likely to set, or at least follow, *de facto* industry-wide standards.

Signs placed at a great distance from a store entrance, either well above or well below eye-level, or obscured through other means such as lettering that blends with its background, are in obvious violation of PIPEDA Principle 3, Consent. An individual cannot give consent to being the object of video surveillance unless she knows such surveillance exists, and she cannot know such surveillance exists unless she can access the notification of surveillance, *i.e.*, unless she can be reasonably expected to see the sign.

4.2.2 Signage non-compliance: lack of information signage text

Where present, signage accompanying the use of video surveillance was usually grossly deficient with respect to the information stated on the sign. According to PIPEDA, notification of the collection of personal information must state:

> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
> (b) the means of gaining access to personal information held by the organization;
> (c) a description of the type of personal information held by the organization, including a general account of its use;
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> (e) what personal information is made available to related organizations (e.g., subsidiaries)" (p. 40).

As video surveillance constitutes collection of personal information, notification of such surveillance is required to include these elements. No signs observed during the fieldwork portion of this project were judged to meet these requirements. For example, the above-noted sign on the entrance to Sq1 (Appendix B, Figs. 2a, 2b, 2c) informs the public only that video surveillance is in use (that is, if one finds and sees the sign, which is unlikely). The sign does not give any contact information, does not describe how to access the personal information collected through surveillance, does not specify what information is being collected or how the information will be used, does not refer to the organization's privacy policies, and does not say with whom the one's personal information may be shared. In other words, the text on this sign does not comply with any portion of the PIPEDA Principle 8, the Openness Principle.

Of the 40 signs observed in fieldwork Phases I and II, 11 (28%) signs contain contact information where an individual can request more information or file a complaint concerning privacy (see Table 2.) In all but one instance, however, this contact information consists of either a phone number or website of a third-party security operator, such as Checkpoint, Chubb or ADT. This might be construed as technically a means for a member of the public to obtain information about the use of video surveillance by the organization, but presumably the third-party security company would not have information with respect to their clients' privacy policies. One sign, that used by the CIBC bank, refers to the company's privacy policy, and directs the public to the main page of the company's website (Appendix B, Fig. 6). While this sign, in terms of wording, iconography, typography, size and placement was the overall closest to compliance that we observed, at least in the private sector, the exclusive reliance on a URL for timely contact is problematic, and in our view, non-compliant. That means, in order to "acquire information about an organization's policies and practices", as stated by PIPEDA, an individual must have an Internet-enabled mobile device on hand and be prepared and able to navigate to the bank's privacy policies, a task that requires considerable time and effort under the best of circumstances. And once one reaches the privacy policy section, it isn't clear about many of the specific, basic questions a surveillance subject may be interested in, such as those regarding monitoring, recording and retention period. Researchers judge this to be contrary to both the spirit of PIPEDA and the specific language of the Openness Principle, which requires organizations collecting personal information give "the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints

or inquiries can be forwarded," and individuals access such information "without unreasonable effort" (p. 40).

4.2.3 Signage non-compliance: vagueness, ambiguity, misleading statements in text of signs

The text of several signs relating to video surveillance is vague or ambiguous, and may either mislead the public about the purpose of video surveillance or present the use of such surveillance as having benefits to the public that do not really exist. Clement and Ferenbok (2011) have observed that signs employed by private companies either "exhibit blunt warnings" or "claim virtues resulting from the cameras such as customer protection and lower prices" (p. 2). Sign used by Home Outfitters (Appendix B, Fig. 7) suggests that the use of video cameras allows the company to maintain low prices by controlling shoplifting: "To protect our customers from rising prices due to shoplifting, this store is guarded by video surveillance". Sears uses similar wording on one of their signs, and also refers to safety: "Shoplifting Affects Everyone / To provide our customers with the best possible value and ensure a safe and secure shopping environment, this store is monitored by / Closed circuit television and trained associates" (Appendix B, Fig. 8). The reference to "trained associates" may give Sears customers the impression that people are actually monitoring their safety and security, although we don't know if that is, in fact, the case. A Costco signs states: "Because we care about your SAFETY & SECURITY this warehouse is monitored by closed circuit cameras" (Appendix B, Fig. 9), although it is not clear how video surveillance improves or promotes customer safety. A sign used by Mark's Work Wearhouse states: "Mark's Uses Surveillance Cameras for the Safety and Security of our Customers and Employees" (Appendix B, Fig. 10). The use of video surveillance is, in fact, for the benefit of the organization only, a means of controlling theft by both employees and the public. On these signs, however, video surveillance is presented as a beneficial, even desirable condition. The explicit mention of personal or public "safety" raises some interesting questions.

The signs of several stores refer to video "monitoring", while others mention "recording," while most say simply, and more vaguely, video surveillance is "in use". Lippert (2009a) notes that "usage," "monitoring," and "recording" are used interchangeably without clear distinctions with respect to the different implications of each word. Lippert notes the ambiguous meaning of "use" and the lack of clarity of the words "monitoring" and "recording". With respect to signs that refer to "monitoring," one may reasonably wonder if actual people are monitoring live feeds of the store. Signage that refers to "safety," as noted above, gives a similar impression. If one falls or is otherwise hurt on the premises, is it reasonable to expect that help will arrive? As noted above, signage that refers to "monitoring" and "safety" gives such an impression, but it may not be true. Organizations that imply safety but don't have the means to respond effectively to safety incidents may be at risk of a failure of "duty to care."

Several stores that employ video surveillance use a generic sign, often depicting a surveillance camera and stating that video surveillance is in use; see, for example, the pictogram at the entrance to Sq1 (Appendix B, Figs. 2a, 2b, 2c). Signs such as these

are too vague and non-informative to be considered PIPEDA-compliant. Some organizations use a small sticker from the third-party operator that handles their surveillance operations, such as Checkpoint, Chubb or ADT (see examples at Appendix B, Figs. 11a, 11b, 11c). Such signs denote the presence of that company's system, but little else.

Separate categories of non-compliance are used in this analysis for ease of discussion purposes. In practice, most signage relating to video surveillance are not compliant with PIPEDA for several reasons. A summary of PIPEDA non-compliance among all signs observed in Phase I and Phase II fieldwork is shown in Table 2, above.

4.3 Responses to verbal questions about privacy policies and practices, Phases I and II

PIPEDA Principle 8, Openness, states:

> An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
>
> 4.8.1
>
> Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.
>
> 4.8.2
>
> The information made available shall include
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
> (b) the means of gaining access to personal information held by the organization;
> (c) a description of the type of personal information held by the organization, including a general account of its use;
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> (e) what personal information is made available to related organizations (e.g., subsidiaries). (p. 42)

PIPEDA Principle 9, Individual Access, states:

> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal

> information and shall be given access to that information. (p. 43)

Thus, any individual requesting information about a company's privacy practices must be able to access such information with relative ease. However, our fieldwork demonstrates widespread non-compliance with these PIPEDA Principles. Many organizations failed to provide information about their privacy practices or their use of personal information collected through video surveillance.

4.3.1 In-store requests for privacy policies and practices refused or ignored

When our field researchers approached store managers to enquire about the privacy aspects of their video surveillance operations, in many cases these organizational representatives said they were not authorized to speak about the company's privacy practices, and would pass along our forms to the corporate officers. If individuals are entitled to "acquire information about an organization's policies and practices without unreasonable effort," as stated in PIPEDA Section 4.8.1 above (p. 42), then responsible employees who deal with the public either should be authorized to discuss those policies and practices with members of the public, or should have a copy of the company's privacy practices available to distribute upon request. However, given that this was not the case – *i.e.*, that most managers claimed they were not authorized to discuss privacy practices – researchers should have been able to easily obtain the information from the organization's corporate office. This was not the case.

In Phase I, despite researcher Kanev's follow-up efforts, 18 out of 45 stores sampled (37%) provided no information about the company's privacy policies and practices. In Phase II, in 99 stores where working video surveillance was observed, 43 store managers (43%) refused to answer questions about company policies regarding video surveillance. In almost all of these cases, managers said they would pass along researchers' requests to the corporate officers. However, researchers often had the impression that managers would not do so. Responses to requests for personal information were received from only 11 (10%) companies.

On a few occasions, store managers asked a researcher to leave the premises. This occurred despite the researcher identifying herself as working on a University of Toronto research project funded by the Office of the Privacy Commissioner of Canada. Given this outcome, we believe a private individual without official credentials or backing would encounter little success when attempting to exercise his or her privacy rights. The implications of these results are discussed in greater detail below.

4.3.2 Responsible employees ignorant about existence of privacy policies and/or PIPEDA requirements

In Phase I, no interviewed employees knew whether or not their company had a policy with respect to video surveillance. Only a few employees had ever heard of PIPEDA, and those that had heard of it were only vaguely aware of its meaning. Only one

manager interviewed in Phase I (2%) reported that she had been briefed on PIPEDA and was aware of the Act's signage requirements.

In Phase II locations where video surveillance was identified, only nine store managers (9%) knew whether or not the company had a policy with respect to video surveillance; 91% of managers did not know if the company had a such policy or refused to answer the question. Managers of 78 stores (79%) were either unaware of PIPEDA or would not say whether they were aware. As above, these figures attest to both widespread ignorance of, and widespread noncompliance with, PIPEDA.

4.3.3 Implications

Store managers' ignorance of organizations' privacy policies, store managers' refusal to speak about organizations' privacy policies, the very low rate of response from corporate offices, and the sometimes hostile response to our interview questions, taken together, demonstrate both widespread ignorance of, and widespread noncompliance with, PIPEDA. These findings demonstrate the need for private sector organizations that interact with the public to provide more training to their front-line staff about the privacy implications of video surveillance and about corporate privacy policies. The poor corporate response rate demonstrates a general trend of non-concern with privacy rights. This underscores our contention that video surveillance is generally seen as having only dimension, that of the benefit to the operator. The privacy rights of the individual being observed – and indeed, even their right to know who is observing them and why – are not considered.

4.4 Outcomes of written requests for personal information, Phases I and II

4.4.1 Non-response rates were very high

A large majority of organizations sampled did not respond to Requests for Personal Information forms in any way. In Phase I, despite the researcher's persistent follow-up efforts, 17 out of 45 companies (37%) either refused to accept a form, accepted the form but never responded, or responded without providing substantive information, then did not respond to further follow-up. In only a few instances were requests for personal information complied with completely and within the 30-day time frame specified by PIPEDA.

In Phase II, when researchers did not follow-up on their requests for personal information, the results were even more stark. Of 99 sites where a Request for Personal Information form was submitted, responses were received from only 11 companies (10%). Of those 11 responses, two companies said they would provide *access to* video images (*i.e.*, the researcher could view an image at the company's offices), one company provided a still image, and only one company provided video images to the researcher.

Did not communicate within the PIPEDA-required 30 days

As outlined above, of 45 organizations contacted in Phase I, 18 organizations (40%) either refused to accept a request for personal information or did not respond to our researchers' request, despite persistent follow-up efforts by both phone and e-mail. In Phase II, where no follow-up was conducted, 88 of 99 companies (88%) either refused to accept the request or did not respond in any way. Obviously, this violates PIPEDA, especially Principle 9, Individual Access, which states:

> Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. (p. 43)

Only 19 companies (13% of Phase I and Phase II combined), did so within the 30-day timeframe mandated by PIPEDA section 8(3). We note that as of the date of submission of this report, a small number of requests for personal information made in Phase II are still under the 30-day time limit.

Figs. 6 and 7 illustrate the outcomes of requests to obtain personal information for Phase I and Phase II fieldwork, respectively. As Fig. 6 demonstrate, 38 of the 45 organizations sampled in Phase I failed to provide any meaningful response to the researcher's request for personal information, despite persistent follow-up by the researcher. In Phase II, seen in Fig. 7, only four of 99 organizations provided any meaningful response, with 88 organizations either not accepting the researcher's request for personal information, or only accepting it without response.

4.4.2 Reasons for refusals to provide video sequences

Among organizations that responded to researchers' requests for personal information, reasons for refusing to provide video sequences fell into a few distinct categories: those that cited security concerns, those that cited concern for the privacy of other individuals in the store, those that requested prohibitively large fees for processing, and those that claimed the requested video had been deleted. Other organizations that partially complied with requests for personal information did so outside the 30-day timeframe stipulated by PIPEDA, or refused to provide video images, but allowed researcher to view images at the company's location.

Refused to provide video, citing security concerns

One of the most troubling stated reasons for organizations' refusals to provide the requested personal information was the claim that it would violate the companies' security interests. Five companies cited security concerns as their reason for refusing the request. The correspondence researcher Kanev received from the chief privacy officer of The Beer Store provides an illustrative example (see Appendix C, Fig. 1). Kanev had been standing in the parking lot outside a Beer Store outlet, photographing signage and video surveillance cameras which were positioned to capture images outside the store. The letter from the privacy officer demanded that Kanev "immediately

cease and desist from this conduct in the future". Thus, a private-sector company that is recording or monitoring public space (the parking lot and the sidewalk outside the store) demands that a member of the public cease taking photographs in that public space. This would seem to be a gross overstatement of security needs, even an over-reaching of private-sector influence on public life.

The privacy officer of The Beer Store stated that the organization would not provide the requested video footage, as doing so would cause the company to "reveal confidential commercial information" regarding security practices. In making this claim, The Beer Store officer cited PIPEDA sections 9(3)(b), "an organization is not required to give access to personal information only if … to do so would reveal confidential commercial information" (p. 12), and 9(3)(c), "to do so could reasonably be expected to threaten the life or security of another individual" (p. 13), explaining that a store employee could be thus harmed. In this instance, a private company that collects individuals' personal information through the use of video surveillance cites PIPEDA to protect their own claimed commercial interests over customer privacy concerns. In our view, this runs counter to both the spirit and letter of Canada's privacy laws. The claim that releasing five minutes of video footage to a customer would either reveal confidential commercial information or threaten the life or security of employee seems to stretch credulity.

All five banks in the Phase I sample refused to provide video footage, each citing security concerns. ScotiaBank, for example, said that access to the requested footage would "divulge security measures" (see Appendix C, Fig. 5). While PIPEDA section 9(3)(c) does exempt organizations from providing access to personal information if "to do so could reasonably be expected to threaten the life or security of another individual," (p. 13) researchers can think of no way in which providing a few minutes of video footage of one individual could possibly threaten the life or security of another. In these instances, it seems that security is being used as an excuse for the denial of privacy rights. Companies like The Beer Store and the banks in our sample use video surveillance, and therefore engage in the collection of personal information, but appear to take little or no responsibility for the privacy implications of those actions. Again, video surveillance is seen as having only one dimension – security – and having no practical significance in terms of privacy.

Refused to provide video, citing privacy concerns

Another reason given for the refusal to provide the requested personal information was the claim that to do so would violate the privacy rights of other identifiable individuals whose images may have been captured in the same footage as our researchers'. Eight organizations responded with this type of claim. Three of those organizations did provide selected still images, saying that they had cropped images of other individuals from the frames. This may be seen as a good-faith effort to comply with PIPEDA requirements.

Although our researchers made every effort to appear in a company's video surveillance without other customers standing nearby, that condition was impossible to guarantee. If other individuals did appear in the requested footage, the eight organizations referenced

here are correct: such footage cannot be released without the permission of each person captured. There is no way to know if the companies' claims were valid, or whether privacy concerns were being used as an excuse to not provide the requested footage; since we could not view the footage, there was no way to verify the claims. In such instances, an inexpensive and readily accessible means of anonymizing images in the video would be a necessary tool for organizations using video surveillance. (See the accompanying report on Video Analytics for a discussion of this possibility.)

Refused to provide video, requested excessive fee

In two instances, organizations claimed that anonymizing images of other individuals captured in the requested video footage would entail considerable expense. One organization, the clothing retailer Le Chateau, claimed such anonymization would cost almost $500 dollars for at most a few minutes of video (see Appendix C, Fig. 2) and wanted assurances that we would cover all costs before they proceeded. PIPEDA Principle 9, Individual Access, states, in part, "an organization shall respond to an individual's request . . . at minimal or no cost to the individual" (p. 41). Thus, requesting an individual cover costs of almost $500 in order to access their personal information violates PIPEDA. As stated above, organizations engaging in video surveillance should equip themselves with the means to anonymize images in video images, in order to comply with potential requests for personal information.

Refused to provide video, claiming footage had been deleted

Nine stores that responded to our requests for personal information claimed that the requested footage already had been deleted when the request was received. A representative of the William Ashley company claimed that the store's surveillance video is overwritten every 24 hours (see Appendix C, Fig. 3); correspondence from Le Chateau claimed "the video will erase in a week time" (see Appendix C, Fig. 2). PIPEDA section 8(8) states:

> an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have. (p. 10)

While PIPEDA does not define "as long as is necessary," it would seem that neither 24 hours nor one week is sufficient time for an individual to access personal information, given that obtaining any response may require days or weeks of follow-up. If these implied retention periods are accurate, it would be a good sign that indicated a spirit of compliance with the data minimization principle, and we certainly are not arguing for longer retention periods to enable individual access to personal video footage, but since we make the request at the moment of video capture, the claim that footage has been deleted indicates that the processing of requests is slow.

Refused to provide video, but allowed researcher to view images at company's location

Five organizations that did not provide the requested video images offered to allow researchers to view still images (three companies) or selected video footage (two companies) at their offices. As PIPEDA states, "The organization shall allow the individual access to this information," (p. 43) viewing video images at a company's location could be interpreted as compliance with PIPEDA. However, requiring an individual to travel during business hours in order to access personal information presents an additional, and potentially prohibitive, obstacle to an individual attempting to access that information. In addition, if video surveillance is in use, selected still images do not constitute the totality of the personal information collected.

One such offer to view a still image came from CIBC. In correspondence to researcher Kanev, a CIBC representative wrote:

> ...the method of access that CIBC will provide you is to produce a copy of the photo and deliver it to a CIBC branch of your choosing to allow you to look at the photo (Appendix C, Fig. 4).

Kanev accepted CIBC's offer to view the image. Although during the course of fieldwork he had spent approximately 10 minutes in a CIBC branch, he was shown only one image of himself. He was not provided with a copy of that image, nor was he allowed to photograph his own image. In this case, the organization that collected personal information is now treating that information as their own property, by refusing to allow the individual to obtain the information.

4.4.3 Positive outcomes, partial and complete

A handful of companies responded to requests for personal information either quickly and completely. One clothing store, Oakley, responded to our request for personal information within a week and prepared video images for our researcher to pick up. Other stores sent detailed privacy polices, usually with reasons for not providing video images.

Among the small number of companies that responded quickly, banks were disproportionately represented. The banking industry, as an industry that is better resourced and more tightly federally regulated than the average retail corporation, may be more attuned to PIPEDA requirements. However, although all five banks responded within the 30-day time frame, none of them provided us with video images.

4.5 Adverse reactions to requests for information about privacy policies or requests for personal information

As this report has noted earlier video surveillance, whether recorded or live monitoring, is considered the collection of personal information. Under PIPEDA, organizations collecting personal information are obligated to answer questions about how that

information will be used. Individuals whose personal information is collected are entitled to request and access that information. There is little, if any, ambiguity about these requirements under PIPEDA. Yet when researchers attempted to exercise their rights in this regard, in most instances (37% in Phase I, 88% in Phase II) were either refused or ignored. In some instances, researchers encountered reactions more troubling than mere refusals. Some store managers were suspicious or hostile, one corporate officer was hostile, and on two separate occasions, researchers were prevented from conducting fieldwork by shopping centre security officers.

During Phase II fieldwork, on four occasions researchers were asked to stop taking photographs and in four separate instances were asked to leave the store or escorted out of the store. As noted above, in response to Phase I research, one company demanded in writing that our researcher “cease and desist” his research. On two other occasions, described in detail below, Phase II researchers were instructed to stop all research by shopping centre security. Again, we note that Phase II researchers politely, in the standard way that they approached all stores, indicated that this was research conducted through the University of Toronto and for the OPC, yet were treated as if they were engaging in sinister, even criminal, activity. Taken together, these incidents strongly suggest that not only will it often be difficult or impossible for members of the public to access information about private-sector privacy policies and practices, and to access their personal information collected by those companies, but sometimes, when attempting to exercise their privacy rights, Canadians can even expect to be harassed, intimidated and threatened.

Fig 6. Outcomes of Request for Personal Information, Phase I

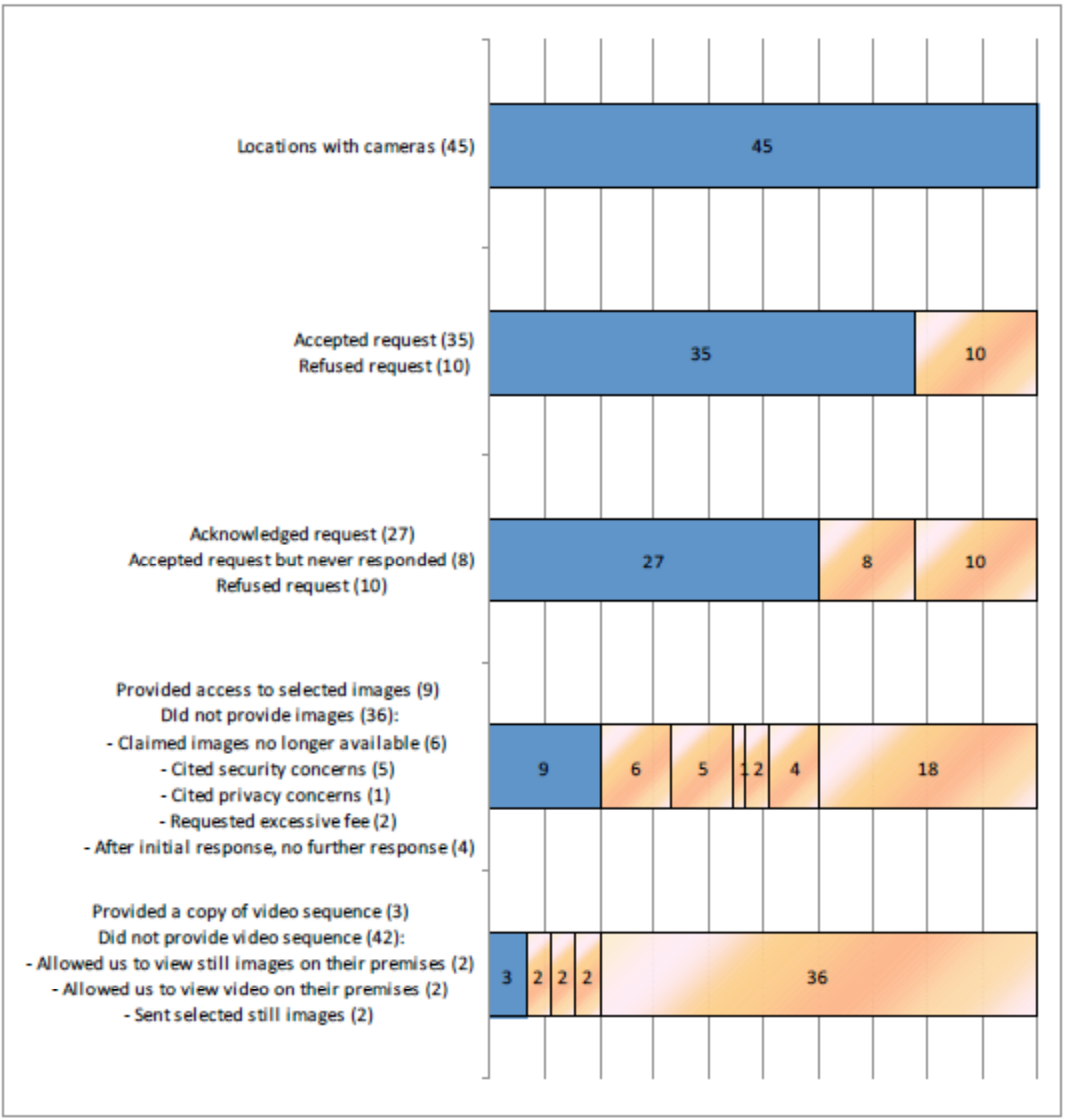
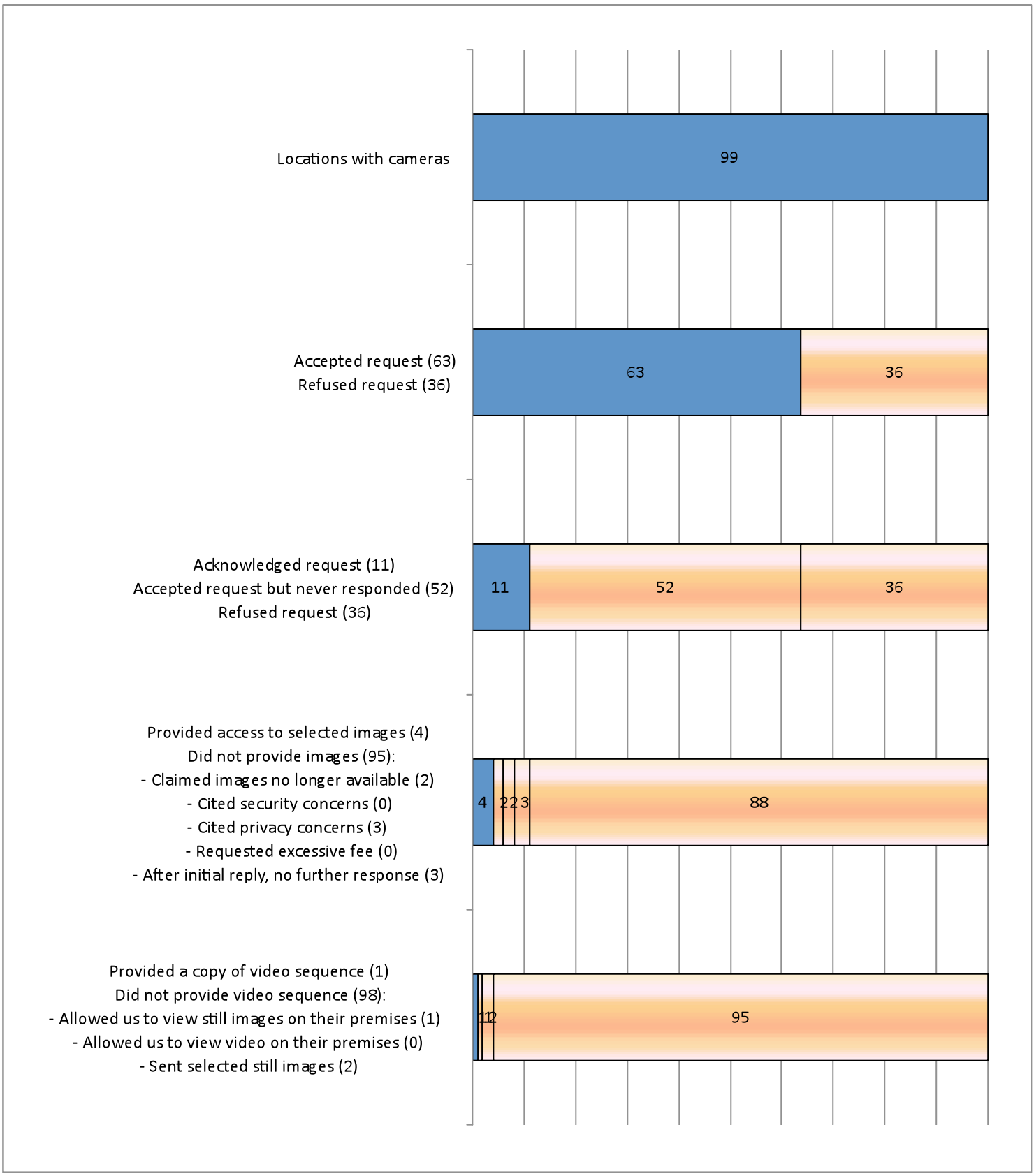


Fig 7. Outcomes of Request for Personal Information, Phase II



4.6 Shopping centre security response to research

On two separate occasions, described in detail in Appendix D, researchers were prevented from conducting fieldwork at a shopping mall by security personnel. Security personnel offered several explanations for prohibiting the work, including mall prohibitions against photography and solicitation, a claimed complaint from a tenant (which researchers believe is unlikely to have occurred), and an agitated response from a store manager who wanted the researcher to surrender her data collection form. Ultimately, our researchers were told that mall security has a right to exclude from the mall any type of behaviour that they wish to, and researchers would have to immediately stop their work.

In the first incident, security personnel had tracked a researcher through video surveillance before confronting her. In the ensuing discussion, the researcher learned that the security manager did not have a clear understanding of PIPEDA as it relates to video surveillance. Although the security manager was aware of the existence of PIPEDA, he did not believe it requires notification of the use of video surveillance. In addition, he offered the opinion that PIPEDA is essentially useless because of its unenforceability. The security officer also stated that in his professional capacity, he believes mall policy supercedes and negates all privacy concerns, and that individuals concerned about privacy should “not go outside”. We find it quite significant that a security manager of Ontario’s largest shopping centre, the second largest mall in Canada, would attest to mistaken and incomplete information regarding PIPEDA, and would express the view that PIPEDA is meaningless.

The security manager told our researcher that mall policy prohibits photography, and that “people get nervous when they’re being photographed,” a claim we find significant. The statement acknowledges that many individuals do not wish to be observed and recorded without their consent. Yet the operators of shopping malls and many other publicly accessible commercial spaces do exactly that. Mall management is constantly – and largely covertly – monitoring and recording the actions of all mall visitors. Since the signage alerting customers to the presence of video surveillance is nearly invisible to anyone who is not purposely searching for it, members of the public are unable to consent to such surveillance. If the security manager is correct – if “people get nervous when they’re being photographed” – then property management’s response to that issue is to not alert those people to the presence of cameras. When leading property managers such as Oxford Properties or Cadillac Fairview actually wish to inform their customers, they use signs such as those directing the public to washrooms, elevators and public transit, seen in Appendix B, Figs. 5a, 5b, and 5c. When management prefers not to inform the public, but is obligated to do so, it meets that obligation with the barest minimum of signage, such as that used on the entrances of TEC and Sq1, seen in Appendix B, Figs. 1a, 1b, 2a, 2b, and 2c. These incidents demonstrate a gross asymmetry between the rights private-sector management claims for itself and those it grants members of the public visiting publicly accessible space.

In Incident 2, after our researcher had collected and recorded her observations, a store manager claimed that the researcher had no right to have done so, and demanded she

surrender her Site Visit Protocol form to the manager. At the same time, in that very store, customers were being tracked by video surveillance without notification and without the provision of any information about the collection of their personal information, who will have access to it, where it is being stored, and so forth. Again we see a gross asymmetry between the rights of the operator of surveillance and the rights of the surveilled.

One often hears of the need for "balance" between the interests of security and the interests of privacy. Our researchers' encounters with mall security officers clearly demonstrate an extreme *imbalance* between these interests in the commercial realm, heavily weighted in favour of security. The researchers see an almost ubiquitous "security over-ride," where claims of security trump any claims of privacy and any claim of security is used to justify any breach of privacy.

5. Conclusions

Based on the findings of this study, one must conclude that video surveillance of the public by the private sector is now a widespread and likely growing practice in the GTA. The near universal use by leading enterprises across various industry sectors, and the adoption by a significant proportion (40%) of the retailers in the two malls we studied indicate that video surveillance has or will soon be the norm, or default option, in the commercial realm. Combined with our observations about the private sector use of cameras outside their stores and often covering public areas, means that we are reaching the point where nearly everyone in urban or shopping areas will be captured on video, often even when they are not entering a store.

This adoption trend is in stark and worrisome contrast to the scant compliance with PIPEDA's notification and personal access requirements. Relatively few surveillance operations have any form of signage (about 30%), and the signage that does exist is far from the minimum standards set by PIPEDA and its related video surveillance guidelines. The findings of this study raise disturbing implications, as both video surveillance penetration and capabilities are expanding rapidly without appropriate public understanding, transparency, oversight or accountability. Individuals who wish to participate fully in society have no choice but to be under near-constant surveillance, while the laws intended to limit the scope of that surveillance are so far largely ignored with impunity.

A major factor that can help explain the current low level of PIPEDA compliance is what can be called a "security over-ride," in which claims of security trump all other concerns, including personal privacy and the privacy rights to which all Canadians are legally entitled and should be able to access. Video surveillance operations appear overwhelmingly to be located within loss-prevention or other security related departments. This reflects an obvious organizational mandate but brings a worldview that typically is directly at odds with key aspects of a privacy protection worldview. In particular, from a security point of view, revealing anything about a security system potentially assists an attacker breach the system. Those who appear to be probing the system, even if simply to ask basic questions about personal information handling, such

as purpose, monitoring, storage, usage, etc. get treated as suspicious and threatening. Unless, the privacy departments of organizations play a strong role, along with security departments, in overseeing video surveillance operations, the security framework will dominate, and privacy considerations will suffer as we have seen.

The authors acknowledge the needs of private sector organizations to maintain adequate security and to take appropriate measures with respect to loss prevention. However, there should be adequate justification for any expansion of those measures, and all measures must comply with legal requirements regarding personal privacy. The very existence of PIPEDA acknowledges the need to circumscribe and limit the collection of personal information, but when it comes to video surveillance in the private sector, as this report shows, PIPEDA is almost always ignored.

Among private-sector employees who interact with the public, including on the managerial level, the degree of awareness of the existence of PIPEDA and its requirements with respect to the collection of personal information through video operation is extremely low. Private-sector organizations need to educate their employees about the implications of video surveillance on personal privacy, on the need for privacy protections, and on the rights of the public to access their personal information. This training could be conceived of as part of the services of third-party surveillance providers, such as Chubb and Checkpoint, which provide video surveillance packages to many Canadian companies, or as part of mandatory managerial training.

Another contributing factor is the lack of public awareness and involvement around video surveillance matters. While video surveillance of citizens raises popular concerns generally, in practice it is very difficult for any individual to do something about it. For a start, few people appear aware that video surveillance is covered by privacy legislation and in the absence of direct and overt harm to themselves are unlikely to attempt to learn about and exercise their rights that they have. If they do initiate a request or later a complaint, they will be faced with a protracted process and in some cases out right hostility, discouraging all but the most ardent. If a complaint is successful, it is largely an isolated event that is unlikely to push any company toward a more PIPEDA-compliant posture. Being more open about surveillance practices and inviting of public queries and personal information requests risks bringing more requests, scrutiny and complaints.

This dynamic creates a self-reinforcing vicious cycle. If people don't know about their rights and how to be effective in exercising them, there is little pressure on organizations to change their low profile. As long as the leading companies maintain a consistently low profile, few citizens will even know how to complain effectively. Short of a highly publicized video surveillance scandal, it would appear that the current situation of widespread non-compliance will not change without some form of external intervention.

This suggests that one route to remediating the current situation is through public education around privacy protection in relation to video surveillance. The OPC could

use its public education mandate to make members of the public more aware of the risks of video surveillance, how to exercise their individual rights and what the obligations of surveillant organizations are in relation to the handling of personal video information. Getting companies to comply with the existing signage requirements, while a limited and partial measure, would also help in educating the public.

More generally it is the regulator's role to balance the interests of private sector security with those of personal privacy. The findings of this report clearly demonstrate that an extreme *imbalance* currently exists, and such imbalance is heavily weighted in favour of private sector security interests, to a degree that virtually negates concern for personal privacy. The OPC needs to take the lead on the side of the public in correcting this imbalance.

Our evidence suggests that PIPEDA non-compliance is sufficiently widespread that it would be appropriate for the OPC to conduct a privacy compliance audit of private sector video surveillance operations. The methodologies of this study provide a useful starting point for such an audit, in terms of assessing actual practices from the point of view of surveillance subjects. An OPC would also be able to investigate aspects that are difficult or impossible in an outsider approach, such as gaining access to the internal policy documents that we have asked for but refused on the grounds of protecting "confidential commercial information".

This study also recommends stronger enforcement of existing privacy laws. While PIPEDA is arguably comparable with the European Union's Data Protection Directive, Canada might consider adopting a more European approach in its implementation, with stiffer penalties and fines on organizations that violate privacy laws. Without them, companies can easily shrug off complaints from individuals.

What may get companies attention is public embarrassment over their lax practices. The OPC could bring greater publicity to the more egregious offenders.

Civil society organizations could also help by assisting individuals in bringing complaints, and aggregating them to give a more cumulative effect.

References

Cadillac Fairview Corporation Limited. (2008). Cadillac Fairview Profile, Toronto Eaton Centre. Retrieved from http://www.cfspace.com/pdf/custom/TORL-8JXJBK_Cadillac_Property_Profile.pdf

City of Toronto. (n.d.). Attraction Highlights. Retrieved from http://www.toronto.ca/attractions/attraction_highlights.htm

Clement, A., & Ferenbok, J. (2011). Mitigating Asymmetric Visibilities: Towards a Signage Code for Surveillance Camera Networks. In A. Doyle, R. Lippert & D. Lyon (Eds.), Eyes Everywhere: The Global Growth of Camera Surveillance. London: Routledge.

Clement, A., Ferenbok, J. & Plataniotis, K. (2010) 'Smart' Private Eyes in Public Places? Video Surveillance Analytics. Toronto: Office of the Privacy Commissioner of Canada.

Directory of Major Malls, 30th ed. (2009). Suffern, N.Y.: MJJTM Publications Corporation.

Globe & Mail Report on Business. (2010, June 18). Rankings of Canada's top 1,000 public companies by profit. Retrieved from http://www.theglobeandmail.com/report-on-business/rob-magazine/top-1000/rankings-of-canadas-top-1000-public-companies-by-profit/article1608779/

Information and Privacy Commissioner of Ontario. (2007, September). Guidelines for the use of video surveillance cameras in public places. Retrieved from www.ipc.on.ca/images/Resources/video-e.pdf

Lippert, R. (2009b). Camera Surveillance, Privacy Regulation, and 'Informed Consent'. In Deisman, Wade, Derby, Doyle, Langlois, Lippert, Lyon, Pridmore, Smith, Walby & Whitson, A Report on Camera Surveillance in Canada Part One. *Surveillance Camera Awareness Network (SCAN)*, 29-40.

Lippert, R. (2009a). Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality. *Social & Legal Studies* 2009(18):505-522.

Office of the Privacy Commissioner of Canada. (2009, April 24). Legal Information Related to PIPEDA. Retrieved from http://www.priv.gc.ca/leg_c/p_principle_e.cfm.

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Officer of the Information and Privacy Commissioner of British Columbia. (2008, March). Guidelines for Overt Video Surveillance in the Private Sector. Retrieved from http://www.oipc.bc.ca/news/rlsgen/Video_Surveillance_Guidelines%28March2008%29.pdf

Oxford Properties. (n.d.). Square One Shopping Centre. Retrieved from: http://www.oxfordproperties.com/leasing/EN/retailFacts.asp?buID=29810

Personal Information Protection and Electronic Documents Act (PIPEDA) (2011, February 9). Consolidation. Retrieved from http://laws.justice.gc.ca/PDF/Readability/P-8.6.pdf

Appendix A: Forms

Appendix A, Fig. 1: Site Visit Protocol, Phase I

Date	Time	Location	Address

Name		Category	

Number of entrances: __ From public space __ From mall space

Is there notification or signage, for each entrance?	
• If yes, what is the proximity of the signage to the entrance (for each entrance)?	
Is there a camera pointed toward or in range of the outside / entrance?	
• Is it likely that the camera captures people outside the immediate retailspace? **Y / N**	
• How many cameras are visible? Fixed Dome Zoom Mini-Dome (Obscured) Other Take image of camera(s), signs and location/setting ___ number of photos taken files: _____	

Job title(s) of store personnel spoken with: _____

What are the purposes for the video cameras?
E.g. Security / public safety / theft prevention / theft detection / prosecution of crimes

What do you do with the images of me you capture via your surveillance cameras?

Is there live monitoring of images? **Y / N / Don't know**
In the store? Remotely?

Is there recording of video? **Y / N / Don't know**
- If Y, for how long?
- Where is this storage located? in the store? Elsewhere?

Is your surveillance cameras system operated by exclusively by your company, or is there a third party operator?
What is the name of this operator?

Under what circumstances are captured images turned over to the police?
- At the store's initiative (eg after a theft or other incident)? **Y / N / Don't know**
- At police request? **Y / N / Don't know**
- Have eithertypes of situation occurred? **Y / N / Don't know**

Does your store havea policy for handling video images? **Y / N / Don't know**

Are you aware of PIPEDA signage requirements? **Y / N / Don't know**

Notes: (e.g. contact info for other corporate personal, notes on the reaction by staff…)

Left a Request for stored personal information with _____ **Y / N** **#**_____
(mention job title of person if different from the above).

Appendix A, Fig. 2: Request for Personal Information, Phase I

Request for Personal Information

Name of Organization: **Address:**

_____ _____

This is a request for personal video information in the possession of your organization, pursuant to the Personal Information Protection and Electronic Documents Act (PIPEDA). (See reverse for relevant provisions.)

In particular, please provide:

- all personally identifiable information derived from video surveillance images and/or recordings of my visit to your organization today during the time period from _____ to _____ (A.M. / P.M.),
- an account of any use or disclosure of my personal information, including my images, and
- all information derived from my visit, including the results of video analytics.

Name of person making request: _____

Physical description: _____

_____

If you require additional information to identify me, you may contact me at the email address below. Please send the information to the address below.

Name: _____

Email: video.privacy.issues@gmail.com

Address: Information Policy Research Program
Faculty of Information
University of Toronto
45 Willcocks Street, Room 326
Toronto, Ontario, M5S 1C7

Signature: _____

Appendix A, Fig. 3: Site Visit Protocol, Phase II

Date:	**Time:**	**Organization / Industry:**	**Address:**

Type of Location: (e.g., interior/exterior, ground floor/upper floor, etc.)	**Number of entrances:** **- exterior: _____** **- from mall: _____**

Photo File Numbers: (note: interior, exterior, close-up, context)

Number of photos of: ___ camera(s) ___ sign(s) ___ context

Is there signage? **Y** / **N** If yes: □ visible □ obscure

If obscure: □ high □ low □ small □ blend w/ background / Describe:

If yes, is sign seen **before** surveilled space? **Y** / **N / Unclear**

Is there a camera visibly pointed outside the entrance? **Y** / **N**

If yes, is it likely that the camera captures people outside the property? **Y** / **N**

How many cameras are visible? ___ PTZ ___ Fixed ___ Dome ___Mini-dome ___Unclear

1. Job title(s) of store personnel spoken with: _____ Refused ☐

2. What are the purposes of the video cameras? _____ Refused ☐

3. What do you do with the images captured through your surveillance cameras? _____

_____

4. Is there live monitoring of images? **Y / N / Don't know / Refused**

4a. If yes, where? In store ☐ Off-site ☐ Both ☐ Don't Know ☐ Refused ☐

5. Is there recording of video? **Y / N / Don't know / Refused**

5a. If yes, for how long before normal deletion? **_____ hrs / _____ days** / **Don't know / Refused**

5b. Where is storage located? In store or off-site? **Y / N / Don't know / Refused**

6. Are surveillance cameras operated by this company ☐ or by a third party operator ☐? **Don't know / Refused**

6a. Name of operator: _____

7. Are captured images turned over to the police? **Y / N / Don't know / Refused**

7a. At store's request? **Y / N / Don't know / Refused**

7b. At request of police? **Y / N / Don't know / Refused**

7c. Has either type of situation ever occurred? **Y / N / Don't know / Refused**

8. Does this store have a policy for dealing with video images? **Y / N / Don't know / Refused**

9. Are you aware that the Personal Information Protection and Electronic Documents Act requires you to give notice when collecting personal information? **Y / N / Don't know / Refused**

Request for Personal Information left with (name/title if known) _____

Request for Personal Information signed: **Y / N / Refused**

Appendix A, Fig. 4: Request for Personal Information, Phase II

UNIVERSITY OF TORONTO
FACULTY OF INFORMATION

Request for Personal Information

Date: 2011____/___ Seq #: _____

Name of Organization: **Address:**

_____ _____

This is a request for personal video information in the possession of your organization, pursuant to the Personal Information Protection and Electronic Documents Act (PIPEDA). (See reverse for relevant provisions.)

In particular, please provide:

- all personal information derived from video surveillance images and/or recordings of my visit to your organization today during the time period from _____ to _____ (AM / PM),
- an account of any use or disclosure of my personal video information and images, including but not limited to, whether someone may have viewed my live video images, the organizational affiliations of all those who may have had access to my images live or via recording, the organizations that had custody of my images, the normal retention period for stored video images captured in this location, and whether any form of video analytics or other automated processing of my video images was performed,
- an account of the purpose(s) for the collection, use or disclosure of my personal information,
- an account of the circumstances under which my personal video information would be provided to police,
- all information derived from my visit, including the results of video analytics, and
- a copy of any brochures or other information that explain your organization's policies, standards, or codes in relation to video surveillance.

My physical appearance: _____

_____

If you require additional information to identify me, you may contact me at the email address below. Please send the information, preferably in electronic form, to the address below.

Name: _____

Email: video.privacy.issues@gmail.com

Address: c/o Information Policy Research Program
Faculty of Information, University of Toronto
45 Willcocks Street, 3rd floor, Toronto, Ontario, M5S 1C7

Signature: _____

Appendix A, Fig. 5: Camera Inventory Form, Phase III

Video Surveillance Camera Inventory

Street Address or Intersection:	
Number of Cameras:	
Organization (e.g., name of store):	
Type of Location (e.g., retail, residential, office):	
3rd Party Operator, if any:	
Signage Present (Y/N):	
If yes:	**☐ visible ☐ obscure**
If obscure:	**☐ high ☐ low ☐ small ☐ hidden** **☐ covers too large an area** **☐ blend w/ background** **☐ other: _____**
Type of space surveilled:	**☐ public ☐ semi-public** **☐ publicly accessible private space**
	☐ sidewalk ☐ park ☐ public plaza **☐ mall common area** **☐ other: _____**
Text of Sign:	
Notes:	

Appendix B, Fig. 2. Signage on entrance to Square One Shopping Centre

Fig. 2a. Close-up of CCTV portion of sign

Text of sign: “CCTV / Security Surveillance Cameras In Use”

Fig 2b. Entire sign

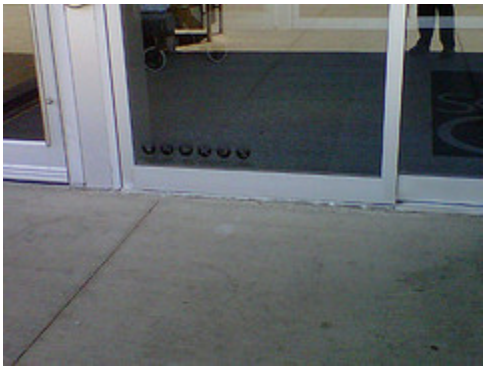


Fig. 2c. Sign in context of entrance

Sign is lower left corner of glass panel, second panel from left.

Appendix B, Fig. 3. Pink store in Square One Shopping Centre

Fig 3a. Close-up of sign

Text of sign: Limited Brands Crime Prevention / Video, Audio, and Recording on Premises / [phone number of security company]

Fig. 3b. Sign in context of storefront

Sign is in lower left corner of left window, near the tail of the dog.

Appendix B, Fig. 4. Generic CCTV sign on HNR Building, Dundas Square, Toronto

Appendix B, Fig. 5. Signage in Toronto Eaton Centre with directions to public transit, washrooms, elevators and other services

Fig 5a. Sign as seen by passerby

Fig. 5b. Sign as seen by passerby

Fig 5c. Signage in typical context

Appendix B, Fig. 6. CCTV Signage on CIBC bank branch, Mississauga

Text of sign, top right: “These Premises Are Under Video Surveillance for Security Purposes. For more information, refer to our privacy policy on cibc.com”

Text of sign, lower left: “Robbery Prevention Program in Place”

Appendix B, Fig 7. Sign in Home Outfitters store, Mississauga

Text of sign: “To protect our customers from rising prices due to shoplifting, this store is guarded by video surveillance”.

Appendix B, Fig 8. Sign in Sears store, Toronto Eaton Centre

Text of sign: “Shoplifting Affects Everyone / To provide our customers with the best possible value and ensure a safe and secure shopping environment, this store is monitored by / Closed circuit television and trained associates”

Appendix B, Fig 9. Sign in Costco store, Mississauga

Text of sign: “Because we care about your SAFETY & SECURITY this warehouse is monitored by closed circuit cameras”

Appendix B, Fig 10. Sign in Mark’s Work Wearhouse store, Toronto Eaton Centre

Text of sign: “Mark’s Uses Surveillance Cameras for the Safety and Security of our Customers and Employees”

Appendix B, Fig 11. Examples of signage of third-party surveillance operators

Fig 11a. Chubb sign on Birks store, Toronto Eaton Centre

Text of sign: “Chubb Video Security / For Customer Protection”

Fig 11b. Checkpoint sign on Addition Elle store, Mississauga

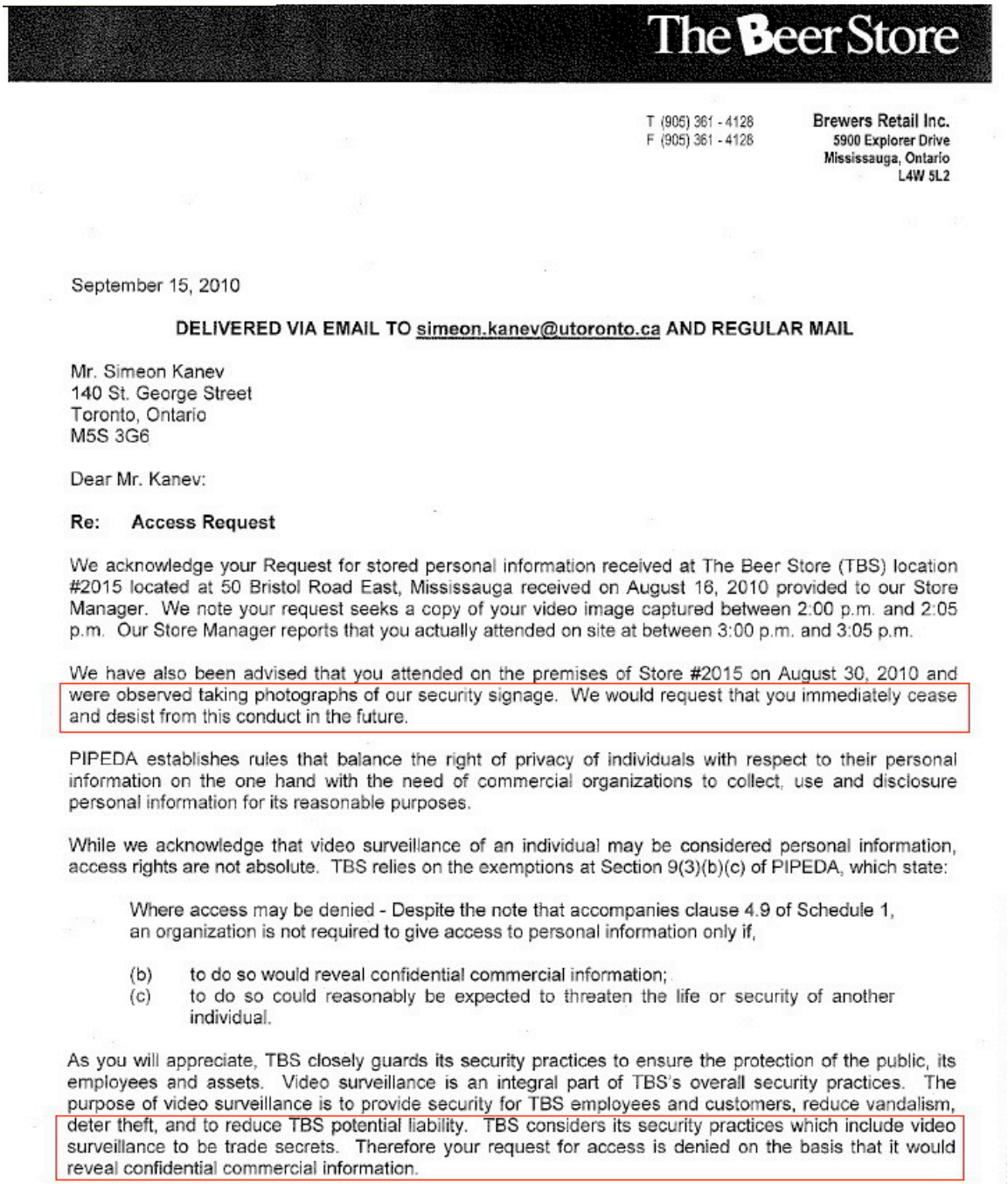
Text of sign: Property Protected By / DIGITAL VIDEO SUREVEILLANCE / From/ Checkpoint Canada Inc. / [company phone number and website]

Fig 11c. INTO Electronics sign, 227 Victoria Street, Toronto

Text of sign: “INTO ELECTRONICS / Providing Electronic Solutions / Electronic Security / Access Control / Video Surveillance / Life Safety / 24 Hour Monitoring and Management, [company website]”

Appendix C: Examples of correspondence with organizations

Appendix C, Fig. 1: The Beer Store



The Beer Store

T (905) 361 - 4128
F (905) 361 - 4128

Brewers Retail Inc.
5900 Explorer Drive
Mississauga, Ontario
L4W 5L2

September 15, 2010

DELIVERED VIA EMAIL TO simeon.kanev@utoronto.ca AND REGULAR MAIL

Mr. Simeon Kanev
140 St. George Street
Toronto, Ontario
M5S 3G6

Dear Mr. Kanev:

Re: Access Request

We acknowledge your Request for stored personal information received at The Beer Store (TBS) location #2015 located at 50 Bristol Road East, Mississauga received on August 16, 2010 provided to our Store Manager. We note your request seeks a copy of your video image captured between 2:00 p.m. and 2:05 p.m. Our Store Manager reports that you actually attended on site at between 3:00 p.m. and 3:05 p.m.

We have also been advised that you attended on the premises of Store #2015 on August 30, 2010 and were observed taking photographs of our security signage. We would request that you immediately cease and desist from this conduct in the future.

PIPEDA establishes rules that balance the right of privacy of individuals with respect to their personal information on the one hand with the need of commercial organizations to collect, use and disclosure personal information for its reasonable purposes.

While we acknowledge that video surveillance of an individual may be considered personal information, access rights are not absolute. TBS relies on the exemptions at Section 9(3)(b)(c) of PIPEDA, which state:

> Where access may be denied - Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if,
>
> (b) to do so would reveal confidential commercial information;
> (c) to do so could reasonably be expected to threaten the life or security of another individual.

As you will appreciate, TBS closely guards its security practices to ensure the protection of the public, its employees and assets. Video surveillance is an integral part of TBS's overall security practices. The purpose of video surveillance is to provide security for TBS employees and customers, reduce vandalism, deter theft, and to reduce TBS potential liability. TBS considers its security practices which include video surveillance to be trade secrets. Therefore your request for access is denied on the basis that it would reveal confidential commercial information.

Further, TBS states that access to a video image with the resulting access to TBS's video surveillance practices could reasonably be expected to threaten the life or security of our employees.

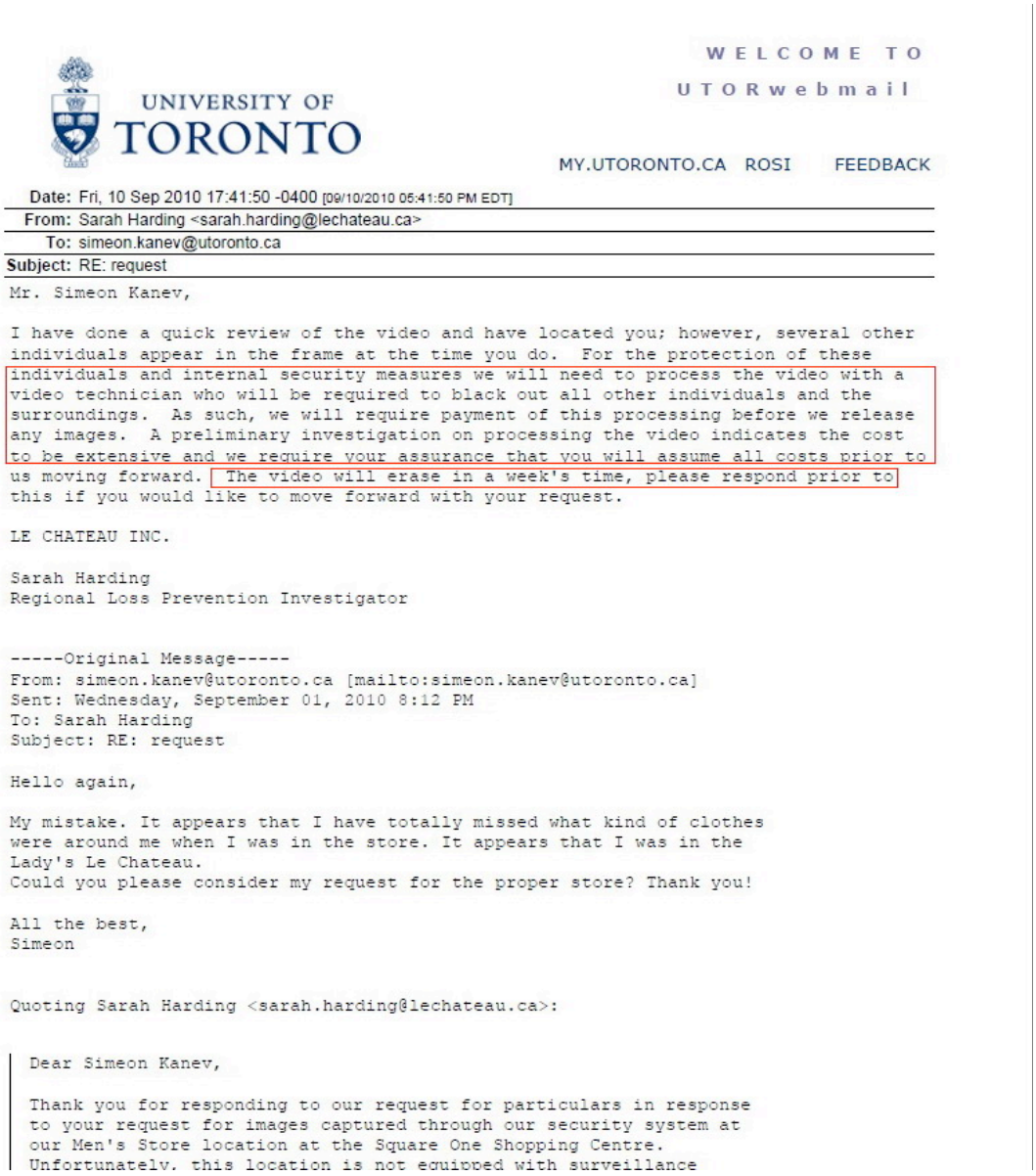
Given the above, your access request is denied in accordance with the provisions of S. 9(3)(b)(c) of PIPEDA.

Yours very truly,

John Crusoe
Chief Privacy Officer
The Beer Store

T- (905) 361-4128
Email – john.crusoe@thebeerstore.ca

Appendix C, Fig. 2: Le Chateau



UNIVERSITY OF TORONTO

WELCOME TO UTORwebmail

MY.UTORONTO.CA ROSI FEEDBACK

Date: Fri, 10 Sep 2010 17:41:50 -0400 [09/10/2010 05:41:50 PM EDT]
From: Sarah Harding <sarah.harding@lechateau.ca>
To: simeon.kanev@utoronto.ca
Subject: RE: request

Mr. Simeon Kanev,

I have done a quick review of the video and have located you; however, several other individuals appear in the frame at the time you do. For the protection of these individuals and internal security measures we will need to process the video with a video technician who will be required to black out all other individuals and the surroundings. As such, we will require payment of this processing before we release any images. A preliminary investigation on processing the video indicates the cost to be extensive and we require your assurance that you will assume all costs prior to us moving forward. The video will erase in a week's time, please respond prior to this if you would like to move forward with your request.

LE CHATEAU INC.

Sarah Harding
Regional Loss Prevention Investigator

-----Original Message-----
From: simeon.kanev@utoronto.ca [mailto:simeon.kanev@utoronto.ca]
Sent: Wednesday, September 01, 2010 8:12 PM
To: Sarah Harding
Subject: RE: request

Hello again,

My mistake. It appears that I have totally missed what kind of clothes were around me when I was in the store. It appears that I was in the Lady's Le Chateau.
Could you please consider my request for the proper store? Thank you!

All the best,
Simeon

Quoting Sarah Harding <sarah.harding@lechateau.ca>:

> Dear Simeon Kanev,
>
> Thank you for responding to our request for particulars in response to your request for images captured through our security system at our Men's Store location at the Square One Shopping Centre.
> Unfortunately, this location is not equipped with surveillance

Appendix C, Fig. 3: William Ashley

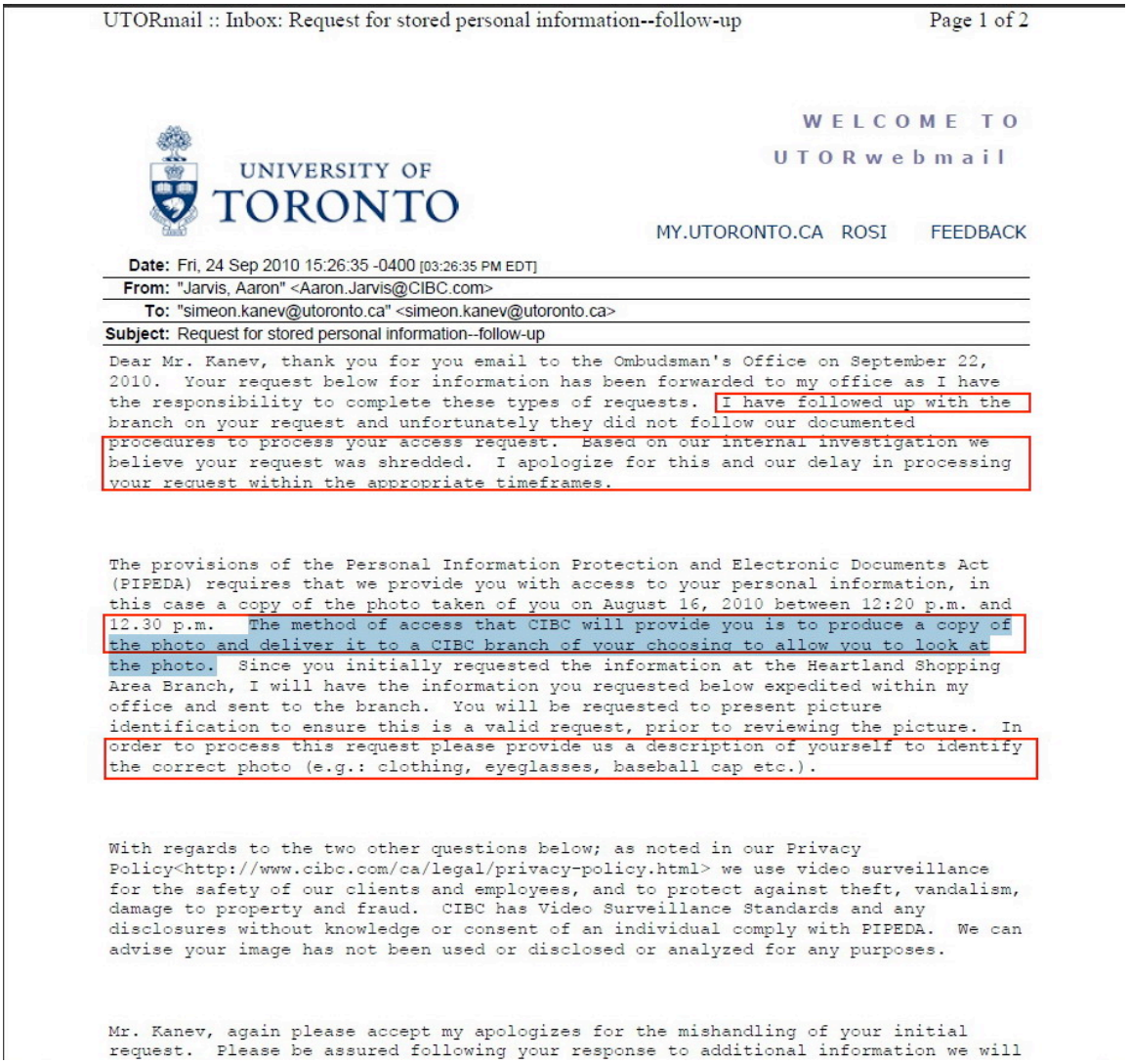
From: Bryna Berman [wma.bryna@gmail.com]
Sent: Tuesday, June 21, 2011 9:36 AM
To: video.privacy.issues@gmail.com
Subject: Wm. Ashley

PLEASE BE ADVISED THAT OUR SECURITY SURVEILLANCE SYSTEM IS OVER-WRITTEN EVERY 24 HOURS. THUS, WE ARE NOT ABLE TO RETRIEVE THE FILES.

IF YOU HAVE ANY QUESTIONS, PLEASE FEEL FREE TO CONTACT ME PERSONALLY AT 416-964-4872

BRYNA BERMAN
WILLIAM ASHLEY CHINA

Appendix C, Fig. 4: CIBC



UTORmail :: Inbox: Request for stored personal information--follow-up Page 1 of 2

UNIVERSITY OF TORONTO

WELCOME TO UTORwebmail

MY.UTORONTO.CA ROSI FEEDBACK

Date: Fri, 24 Sep 2010 15:26:35 -0400 [03:26:35 PM EDT]
From: "Jarvis, Aaron" <Aaron.Jarvis@CIBC.com>
To: "simeon.kanev@utoronto.ca" <simeon.kanev@utoronto.ca>
Subject: Request for stored personal information--follow-up

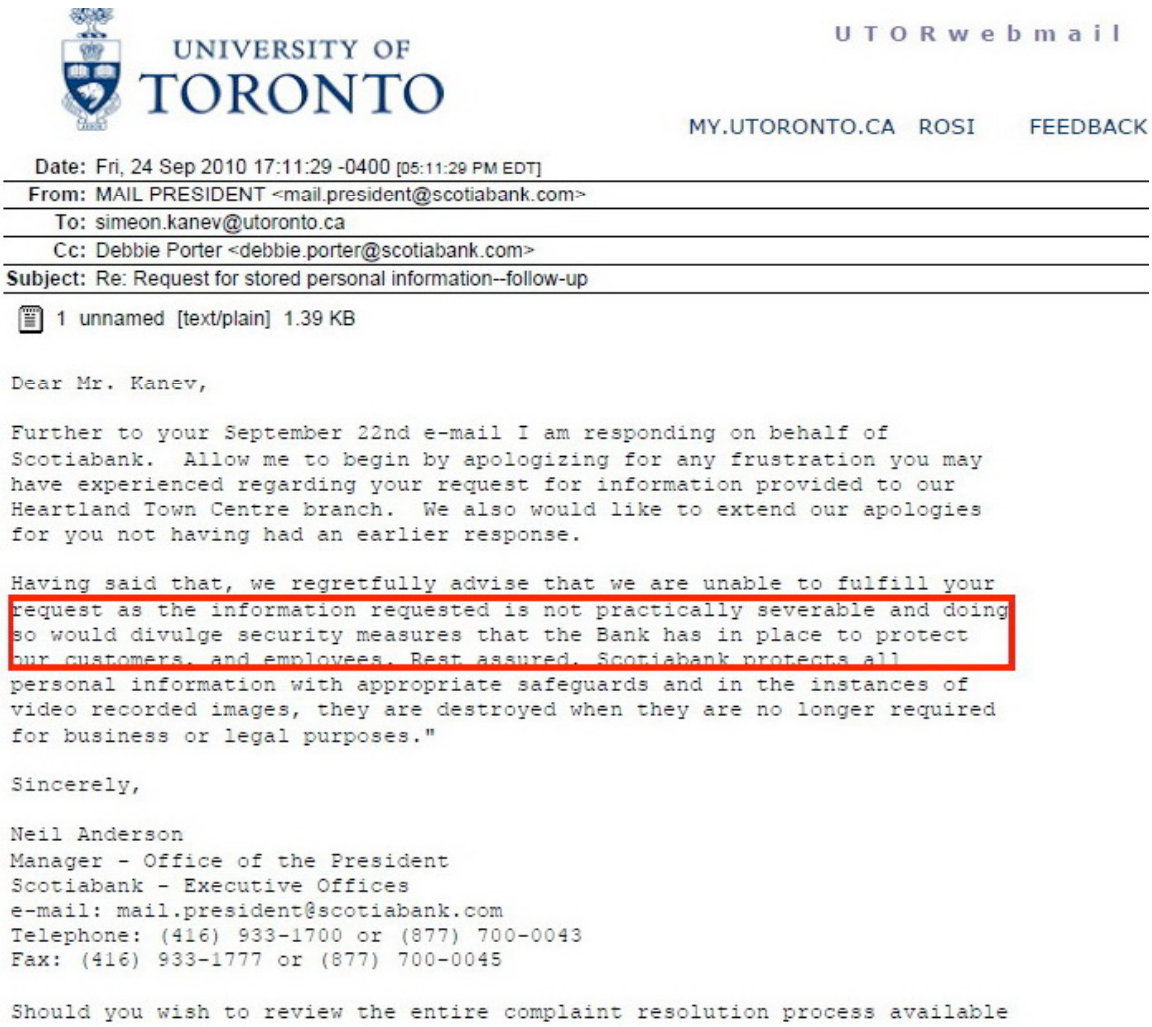
Dear Mr. Kanev, thank you for you email to the Ombudsman's Office on September 22, 2010. Your request below for information has been forwarded to my office as I have the responsibility to complete these types of requests. I have followed up with the branch on your request and unfortunately they did not follow our documented procedures to process your access request. Based on our internal investigation we believe your request was shredded. I apologize for this and our delay in processing your request within the appropriate timeframes.

The provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA) requires that we provide you with access to your personal information, in this case a copy of the photo taken of you on August 16, 2010 between 12:20 p.m. and 12.30 p.m. The method of access that CIBC will provide you is to produce a copy of the photo and deliver it to a CIBC branch of your choosing to allow you to look at the photo. Since you initially requested the information at the Heartland Shopping Area Branch, I will have the information you requested below expedited within my office and sent to the branch. You will be requested to present picture identification to ensure this is a valid request, prior to reviewing the picture. In order to process this request please provide us a description of yourself to identify the correct photo (e.g.: clothing, eyeglasses, baseball cap etc.).

With regards to the two other questions below; as noted in our Privacy Policy<http://www.cibc.com/ca/legal/privacy-policy.html> we use video surveillance for the safety of our clients and employees, and to protect against theft, vandalism, damage to property and fraud. CIBC has Video Surveillance Standards and any disclosures without knowledge or consent of an individual comply with PIPEDA. We can advise your image has not been used or disclosed or analyzed for any purposes.

Mr. Kanev, again please accept my apologizes for the mishandling of your initial request. Please be assured following your response to additional information we will

Appendix C, Fig. 5: ScotiaBank



UNIVERSITY OF TORONTO

UTORwebmail

MY.UTORONTO.CA ROSI FEEDBACK

Date: Fri, 24 Sep 2010 17:11:29 -0400 [05:11:29 PM EDT]
From: MAIL PRESIDENT <mail.president@scotiabank.com>
To: simeon.kanev@utoronto.ca
Cc: Debbie Porter <debbie.porter@scotiabank.com>
Subject: Re: Request for stored personal information--follow-up

1 unnamed [text/plain] 1.39 KB

Dear Mr. Kanev,

Further to your September 22nd e-mail I am responding on behalf of Scotiabank. Allow me to begin by apologizing for any frustration you may have experienced regarding your request for information provided to our Heartland Town Centre branch. We also would like to extend our apologies for you not having had an earlier response.

Having said that, we regretfully advise that we are unable to fulfill your request as the information requested is not practically severable and doing so would divulge security measures that the Bank has in place to protect our customers, and employees. Rest assured, Scotiabank protects all personal information with appropriate safeguards and in the instances of video recorded images, they are destroyed when they are no longer required for business or legal purposes."

Sincerely,

Neil Anderson
Manager - Office of the President
Scotiabank - Executive Offices
e-mail: mail.president@scotiabank.com
Telephone: (416) 933-1700 or (877) 700-0043
Fax: (416) 933-1777 or (877) 700-0045

Should you wish to review the entire complaint resolution process available

Appendix D "Security versus Privacy" research incidents in a major shopping mall

Incident 1:

The first incident took place during fieldwork in June, 2011. Researcher Laura Kaminker was in a store, talking to some store employees about matters unrelated to the project. Kaminker was approached by two male security officers, who asked, "Are you Laura? Come with me, please." They escorted Kaminker out of the store. One of them was holding a Personal Information Request form that Kaminker had left in a store earlier that day.

The men claimed that they had received complaints from mall tenants; they claimed Kaminker was intimidating store managers, and that store managers had reported being frightened by Kaminker's questions. Kaminker – who is 50 years old and 5'1" tall, and had conducted several cordial, friendly interviews that day – thought it unlikely that anyone had found her intimidating.

The security manager responded, "It's not your manner that's intimidating, it's the fact that you are asking questions. I'm sure you can appreciate why that scares people." Kaminker said that she did not understand why anyone would be afraid of a brief survey that they were free to decline.

The security manager then referred to the mall's policy against solicitation. When Kaminker said she was not selling anything, the security manager used the example of religious solicitation as non-commercial interaction which is prohibited at the mall. Kaminker reiterated that she was not soliciting, she was collecting data.

The security manager then referred to the mall's policy against photography, saying, "You're taking photographs. We have a strict no photography policy in the mall." Kaminker replied that such a policy was interesting given mall visitors are under constant surveillance by management.

The security manager replied, "People get very nervous when they're being photographed. Especially if there are children present. People don't like to see people with cameras walking around."

Kaminker noted that she was very careful to not capture other mall visitors in her photographs, that the photographs were of storefronts, cameras and signs only. She then offered to conduct the remainder of the research without photography. In response, the security manager said, "Photography or not, it's my responsibility to control what happens in this space. It's my right to do so, and I'm telling you to stop doing what you're doing."

Kaminker asked how the security officers had found her inside the store. They replied, "On video. We've been tracking you." She asked if that meant that no tenant had

actually complained about the research. The security manager said, “I can’t tell you that.” Kaminker does not believe that any tenant complained about her research.

Both security officers looked at a letter from Professor Clement confirming that Kaminker was working on research funded by the OPC; they asked for a copy, which Kaminker said she would email. The security manager said he would need permission from Oxford Property’s national office and legal department in order for research continue at mall. When Kaminker said that project researchers had visited the mall on two other occasions, and had completed fieldwork on major shopping mall, the security manager was extremely surprised.

On previous fieldwork visits to the mall, employees in the mall’s security office would not answer any of the standard interview questions. During Incident 1, Kaminker asked about the mall’s surveillance policies, effectively conducting a partial interview; the security manager answered all her questions. Kaminker and the security manager talked about the project, about PIPEDA requirements, the unenforceability of PIPEDA, the current capability of video surveillance, video analytics, and other aspects of video surveillance.

During this discussion, Kaminker asked the security manager about the lack of PIPEDA-compliant signage in the mall. The security manager said that PIPEDA does not require signage. When Kaminker noted that PIPEDA does indeed require notification of the collection of personal information, and that video surveillance is considered such collection, the security manager said, “Our defense is that if you go out in public, you should have the expectation that your actions are being watched. If you don’t want to be surveilled, don’t go outside.” At one point, the security manager noted that even if the mall’s notification is not PIPEDA-compliant, individuals who find that problematic have little recourse. He said, “What are they going to do about it? File a complaint. Big deal.”

After some discussion, Kaminker told the security officers that she needed to remain in the mall until her ride was expected, and did not want to be watched the entire time. The security officers made a point of telling her that she was not being asked to leave the mall, merely to stop conducting research.

Incident 2:

Immediately after Incident 1, Professor Clement spoke to Ms. Celia Hitch, legal counsel for Oxford Properties, the mall management firm. Hitch indicated that she could see no problem with the research, but suggested discussing this with Jean-Marc Rouleau, general manager of the Shopping Centre, which he did. Two days later, Professor Clement provided Mr. Rouleau with information and supporting documentation about the research project, mentioning the plan to resume research later in the week. Mr. Rouleau agreed to forward the information to mall tenants, giving them the opportunity to opt-out of the research. Professor Clement did not receive any opt-out requests, from Mr. Rouleau or any mall stores.

Researcher Roxanna Dehghan returned to the mall as scheduled several days later. It was her third fieldwork visit to the mall. Researcher Dehghan was interviewing the manager of a store in the usual manner; the manager had prefaced the interview by saying that she could not answer questions about the surveillance system because "they pertain to sensitive information," but agreed to be interviewed. Once Dehghan began the interview, the manager refused to answer any questions, although she did acknowledge that she is personally aware of PIPEDA requirements.

Dehghan then began to explain the Request for Personal Information form and its use. The manager became agitated and requested Dehghan give her the Site Visit Protocol form (the record of their interview). The manager may have misunderstood the purpose of the interview and mistakenly believed Dehghan was selling something. Dehghan explained that she was merely requesting that the Request for Personal Information be given to the store's corporate office. She explained that the form contained Dehghan's name and contact information, as well as contact information of her research supervisor.

The manager became agitated and again requested that Dehghan give her the Site Visit Protocol form. Dehghan explained that she needed the form in order to record the data she has just collected (*i.e.*, the answers to their interview). Dehghan and the manager argued over the survey form. The store manager asked if mall management was aware of the research; Dehghan replied that the mall general manager knew about the project.

The store manager called security. When a security officer arrived, the store manager gave the security officer an inaccurate account of the research, claiming that Dehghan said the survey was mandatory and that she was with the Office of the Prime Minister. The security officer instructed Dehghan to give the Site Visit Protocol form to the store manager. Dehghan offered to make a copy of the form for the manager. The manager became very agitated and insisted that she needed the original form.

The security officer asked Dehghan about her research. In her explanation, Dehghan mentioned that she and a colleague had made previous visits to the mall during the course of this project. The security manager called this information "hearsay". Dehghan and the security guard argued about the research. The security guard asked Dehghan for identification; she produced her student ID card. The security guard then asked Dehghan for her driver's license; she refused, as is her right. Eventually the security guard notified the security office that Dehghan was being "uncooperative" and "hostile". Another man joined them, presumably a security officer, although he did not produce identification. This man accused Dehghan of soliciting and told her to leave the mall. Both security officers claimed to be unaware of a similar incident the previous week (*i.e.,* Incident 1, described above) or of any correspondence between Rouleau and Clement. The incident ended when Dehghan agreed to leave the mall**.**

Appendix E: PIPEDA Compliance of Signage Observed in Phases I and II.

The following 6 pages consist of the Excel spreadsheet, *PIPEDA Compliance of Phase I and Phase II Signage*

The latest version can be viewed, likely more conveniently, at:

https://docs.google.com/spreadsheet/ccc?key=0AuE2koOsSVEYdFdleHFOMzJXckpGb0xSWHl6Ulc5Y0E&hl=en_US#gid=0

PIPEDA Compliance of Phase I and Phase II Signage									
	Details		Visibility/Legibility						
	Text of Sign	Flickr URL	Size (Large enough to spot easily)	Placement (Readable before entering surveilled area)	Location (On all normal entry routes)	Contrast (Easily discernable from background)	Contact Info (present and immediately actionable)	Purpose (Specified and appropriate)	Responsible party(ies) (Identified, for surveillance operation and for privacy compliance)
Addition Elle	Property Protected By Digital Video Surveillance	http://bit.ly/nz	N	N	N	Y	Y**	N	N
Banana Republic TEC	This store is protected by video surveillance equipment	http://bit.ly/qI	N	N	N	N	N	N	N
Banana Republic Sq1	This store is protected by video surveillance equipment	http://bit.ly/r6	N	N	N	N	N	N	N
Beer Store, The	Premises protected by CCTV surveillance system	http://bit.ly/oA	N	N	N	Y	N	N	N
Best Buy	These premises are equipped with video surveillance	http://bit.ly/rs	Y	N	N	Y	N	N	N
Birks (Sq1)	Chubb Video Security for Customer Protection	http://bit.ly/qE	N	N	N	N	Y**	N	N
Birks (TEC)	Chubb Video Security for Customer Protection	http://bit.ly/qE	N	N	N	N	Y**	N	N
Blockbuster	This store is protected by Closed Circuit Camera	http://bit.ly/rqi	N	N	N	N	N	N	N
Cadillac Fairview (TEC)	As Part of Our Management Services Cadillac Fairview Uses Closed Circuit TV at This Property	http://bit.ly/rd4	N	N	N	N	N	N	Y
Canadian Tire (TEC)	Notice to Customers, we respect the privacy of our customers video surviellance are used on these premises for the protection of our customer and our businesses. Except as requireed by laws or as part of a legal investigation the images are for internal use only	http://bit.ly/oh	Y	N	N	Y	N	N	N
CIBC	These Premises are Under Video Surveillance for Security Purposes	http://bit.ly/p3	Y	Y	Y	Y	Y**	Y	Y
Costco	Because we care about your … SAFETY&SECURITY this warehouse is monitored by closed circuit cameras	http://bit.ly/ple	Y	N	Y	Y	N	N	N
Famous Players Cinema	Notice: These Premises are monitored by video surveillance	http://bit.ly/r0l	N	N	Y	N	N	N	N
GAP	Warning closed circuit television (www.checkpoint.com)	http://bit.ly/odEmpg	Y	Y	Y	Y	Y**	N	N

GNC	Warning Closed Circuit Television on Premises	http://bit.ly/r1	Y	N	Y	Y	Y**	N	N
Grand & Toy	Security Cameras in Use on these premises	http://bit.ly/rg	Y	N	N	N	N	N	N
Her World	Warning these premises protected by surveillance systems	http://bit.ly/q2	N	N	N	Y	N	N	N
Home Outfitters	To protect our customers from rising prices due to shoplifting, this store is guarded by video surveillance	http://bit.ly/nx	Y	N	N	N	N	N	N
Lenscrafters	Warning! These premises protected by closed circuit television system (1888846cctv)	http://bit.ly/oa	N	Y	Y	Y	Y**	N	N
Loblaws	Please be advised, our store has video surviellance equipement designed for our customer's protection and to help keep prices low	http://bit.ly/p1	Y	N	N	Y	N	N	N
Mark's Work Wearhouse	Mark's uses surveillance cameras for the safety and security of our customers and employees	http://bit.ly/o3	Y	Y	Y	N	N	Y	N
Metro	This property is protected by surveillance system with remote viewing capabilitiy	http://bit.ly/qV	N	N	N	N	N	N	N
Oxford Mgmt (Sq1)	CCTV security surveillance cameras in use	http://bit.ly/pI7	N	N	Y	N	N	N	N
Pink	Video. Audio. and Recording on Premises (and) This store is under video surveillance	http://bit.ly/nM	N	Y	Y	N	Y**	N	N
RBC	Some areas of this building may be monitored by video or other means for safety and security	http://bit.ly/ra	N	N	N	N	N	N	N
Reitman's	Private property protected by Anti-shoptheft systems EAS – CCTV	http://bit.ly/qlU	N	N	N	N	Y**	N	N
Sears (Sq1)	Shoplifting affects everyone. To provide our customers with the best possible value and ensure a safe and secure shopping environment, this store is monitored by closed circuit television and trained associates	http://bit.ly/oe	Y	N	N	Y	N	N	N
Sears (TEC)	Some areas of this building may be monitored by video or other this area is monitored by closed circuit television	http://bit.ly/oe	Y	N	N	N	N	N	N
Sephora (TEC)	For Secutiy and safety purposes, this store is monitored by video camera. for information call 1-514-932-1616 ext. 0	http://bit.ly/q6	Y	Y	Y	Y	Y**	Y	N
Sephora (Sq1)	For Secutiy and safety pruposes, this store is monitored by video camera. for information call 1-514-932-1616 ext. 0	http://bit.ly/q6	Y	Y	Y	Y	Y	Y	N

Smart Set	Property Protected By Digital Video Surveillance	http://bit.ly/pp	N	N	N	N	N	N	N
Staples	Private property protected by Digital Video Surveillance by Checkpoint	http://bit.ly/nz	N	N	N	N	N	N	N
Swiss Chalet	Attention: security cameras are in use at this restaurant	http://bit.ly/q5	Y	Y	N	Y	N	N	N
Telus	These premises use video surveillance for security purposes	http://bit.ly/nL	N	N	N	N	N	N	N
Tilley Endurables	Security monitors are in place for everyone's protection	http://bit.ly/nD	N	N	N	Y	N	N	N
Tim Horton’s	Notice Roberry prevention program in effect for the safety and security of our customers and employees, this restaurnt is subject to video surveillance limited cash on hand	http://bit.ly/nJ	Y	N	Y	Y	N	N	N
Toys Toys Toys	For security purposes, this store is on 24 hour video surveillance	http://bit.ly/oM	N	N	N	N	N	N	N
Trade Secrets (SQ 1)	24 HOURS Warning This property is protected by Video Surveillance	http://bit.ly/on	Y	Y	Y	Y	N	N	N
Winners	Closed circuit television cameras are in use in our stores. Images are recorded for the purposes of the detection and prevention of crime	http://bit.ly/nM	N	N	N	Y	N	N	N
Zara	Video Surveillance	http://bit.ly/qHtJwh	N	N	N	N	N	N	N

Content			
Live Monitoring (indication of whether this is occurring)	Recording (Indication of whether this is occurring)	Recording (Indication of duration)	Video analytics (Indication of whether any automated processing is occurring)
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N

N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	Y	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N

N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N
N	N	N	N