Private Sector Video Surveillance in Toronto: Not Privacy Compliant!

Andrew Clement
Faculty of Information
University of Toronto
140 St George Street
Toronto, ON M5S 3G6 Canada
andrew.clement@utoronto.ca

Joseph Ferenbok
ICCIT, KMDI
University of Toronto
CCT Building, 3359 Mississauga Rd
Mississauga, ON L5L 1C6 Canada
joseph.ferenbok@utoronto.ca

Roxanna Dehghan, Laura Kaminker & Simeon Kanev
Faculty of Information
University of Toronto

ABSTRACT
We report on the findings of a fieldwork study conducted on private sector video surveillance and signage in the Toronto area. The presence and operation of over 140 video surveillance camera schemes by large service providing corporations, in 2 major shopping centres and visible from public areas in downtown Toronto is documented. We analyse the data generated in relation to compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA), the prevailing privacy law that governs such video surveillance operations. We find widespread non-compliance with PIPEDA, especially with regard to Principles 8 - Openness, and 9 - Individual Access. We explain this finding as resulting from a form of "security over-ride," in which claims of security trump other concerns, including personal privacy. We propose stronger privacy awareness and enforcement around private sector video surveillance.

General Terms
Management, Security, Human Factors, Standardization, Legal Aspects

Keywords
Privacy, video surveillance, regulation, PIPEDA, private sector

1. INTRODUCTION
Anyone with an eye for video surveillance cameras walking around the popular areas of Toronto will have little trouble finding them in abundance. If they have a basic knowledge of the Personal Information Protection and Electronic Documents Act (PIPEDA), the privacy legislation that governs handling of personal information in the private sector, they will similarly have little trouble concluding that most video surveillance operations are not compliant with the notification or openness requirements of PIPEDA.

This provided the starting point for our research team, based at the University of Toronto, to conduct fieldwork seeking to document the use of video surveillance and to test such surveillance for relative compliance or non-compliance with PIPEDA requirements. The main research questions we asked were:

- How extensive is video surveillance in the private sector in the Greater Toronto Area (GTA)?
- Are private-sector video surveillance operators aware of PIPEDA? Are they compliant with PIPEDA requirements?
- What notification do video surveillance operators provide, both publicly and on request, about their use of such surveillance?
- What can an individual expect in terms of the collection of their personal information? If an individual attempts to exercise her rights under PIPEDA, will her rights to request and access that information be respected?

Whereas research into video surveillance (aka closed circuit television (CCTV)) is long standing in Europe [7], and particularly in the UK [10], empirical studies of video surveillance in Canada are relatively recent. Much of it is sociological, involving close examination of several case studies of particular CCTV schemes in municipal settings [8]. The closest work to our own comes from the work of the Surveillance Camera Awareness Network research studies. [4] Within this body, Lippert's is one of the few that looks specifically at camera signage [9]. We also build on our own prior work in proposing PIPEDA compliant video surveillance signage schemes [2] and analyzing the privacy implications of the shift from conventional analog CCTV to digitally networked video surveillance schemes, with their growing prospects for incorporating automated video analysis techniques [6]. The main contributions of the work reported here derive from the empirical focus on private sector installations and their PIPEDA (non)compliance.

2. VIDEO SURVEILLANCE AND PRIVACY
The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal legislation governing the use of video surveillance in the private sector, including in Ontario and all other provinces, except for Alberta, B.C and Quebec which each have their own, substantially similar legislation. Private-sector organizations must comply with several PIPEDA principles when engaging in the collection, use, disclosure, retention, and destruction of personally identifiable information.

iConference 2012, February 7-10, 2012, Toronto, Ontario, Canada
ACM 978-1-4503-0782-6/12/02.

The Office of the Privacy Commissioner of Canada [12] has determined that both video recordings and real-time video surveillance without recording constitute the collection of personally identifiable information; thus, the rights set forth in PIPEDA apply. PIPEDA 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. These requirements are further spelled out in Guidelines for Overt Video Surveillance in the Private Sector developed jointly by federal and provincial privacy authorities regarding video surveillance in the private sector [12].

There are several of the Fair Information Practice Principles [5,11] incorporated within PIPEDA that directly apply to the collection of personal information through the use of video surveillance. The two are most directly relevant to our study are Principles 8, and 9, excerpted here:

> **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 Principle 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).

The Individual Access Principle 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. Other principles relevant to our study include: Principle 1, Accountability; Principle 2, Identifying Purposes; Principle 3, Consent; and Principle 5, Limiting use, disclosure, and retention.

3. FIELDWORK METHODOLOGY

We approached the fieldwork in three distinct phases. The first phase targeted the largest, most prominent firms in the private sectors that 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 Greater Toronto Area (GTA) – the Eaton Centre (TEC) and Square One in Mississauga, both very popular with consumers. The third phase targeted cameras in downtown Toronto 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 Sampling

3.1.1 Phase I- Industry leaders

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*. 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 the GTA and Ontario. 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 researcher Kanev'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.

3.1.2 Phase II - Major Shopping Malls

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. Sq1 is the largest shopping centre in the province of Ontario [13] and the second largest indoor mall in Canada [3]. Both TEC and Sq1 are official landmarks and promoted by their respective cities as tourism destinations; both receive millions of visitors each week [1].

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. In all, the Phase II sample comprises 101, out of approximately 300, locations in Sq1 and all 158 locations in TEC, a total of 258 locations. This also includes the common areas of both shopping centres. Phase II research tested the prevalence of video surveillance in the private sector, as well as the other aspects mentioned in the case of Phase I

3.1.3 Phase III - Open Street Surveillance

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 http://surveillancerights.ca. As this phase of the work is still on-going, we will not report further on it here, beyond noting that the results so far in terms of quality and lack of signage is consistent with the findings for the previous two phases.

3.2 Site visit methods

Fieldwork for Phase I began in July 2010 and was completed by October. Field work for Phase II began in April 2011 and was completed by July 2011. Both adopted a very similar observation, enquiry and recording methods.

For each location in the sample, the researcher prepared for the site visit by recording standard data on a Site Visit Protocol form: 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 http://www.flickr.com/groups/1233129@N25

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.

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. 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. 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.

To better replicate the experience of an 'ordinary citizen', in the Phase I study the researcher, Kanev, a clean shaven male graduate student in his twenties, presented himself as would a potential customer, mentioning his research interest only if asked for reasons for his visit or for making the information request. Following the visit, 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 prompt a response, the researcher would wait an additional 30 days, then send a second reminder. No further reminders were sent.

In Phase II, researchers Dehghan and Kaminker, both female graduate students of differing ages visiting sites individually, immediately identified themselves as assistants in a University of Toronto study funded by the Office of the Privacy Commissioner. Although such identification appears to have helped them in gaining the attention of store managers, it made little difference in the willingness to accept requests for personal information, nor did it assist on the occasions when shopping centre management took an adversarial approach to the research project. Also in contrast to Phase I, no follow up was done in the case of non-response. This had a dramatic dampening effect on the

communication – less than 20% of the organizations that accepted the Personal Information Request form responded.

4. FINDINGS

The various aspects of the field each produced notable findings, which we will consider in the order in which they were encountered in the research process. We start by highlighting in turn the presence of cameras, prevalence of signage, PIPEDA compliance of signage, responses to verbal questions about privacy polices and practices and finally response to written requests for personal information. Across all these aspects, we find evidence of PIPEDA compliance sparse to non-existent.

4.1 Presence of video surveillance cameras

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 252 locations (38%). Of the locations where video cameras were observed (including 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.

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.

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.

4.2 Presence of notification of video surveillance

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 provide surveillance subjects with meaningful information about video surveillance practices is usually lacking. Official Privacy Commission guidelines mentioned earlier clearly state signage is necessary, and the basic ingredients of what such signage should contain. 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. 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. 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.

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, mentioned earlier.

4.3 Compliance of signage with PIPEDA

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, 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, including the size and placement of the sign, relate to both Principle 2, Identifying Purposes, and Principle 3, Consent, as well as PIPEDA Principle 8, the Openness Principle, all quoted above.

In both Phase I and Phase II samples, we analyzed every sign observed. None we judged to be fully compliant with PIPEDA requirements. Of the 16 signs observed in Phase I, 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 stated 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". See the Flickr group mentioned above for access to all the images of signs.

In Phase II, 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 approaching the store, requiring a careful search for signs, as our researchers needed to do. Of the 26 signs observed, most were very small, placed either far above or far below eye level, designed to blend in with the background and otherwise barely visible. 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.

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

PIPEDA Principles 8, Openness, and 9, Individual Access, imply that 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.

4.4.1 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 (11%) 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.

4.4.2 Responsible employees ignorant about existence of privacy 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 such a policy or refused to answer the question. Managers of 78 stores 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. This underscores our contention that video surveillance is generally seen as having only one 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 seldom considered.

4.5 Outcomes of written requests for personal information

4.5.1 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 (11%). 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.

4.5.2 Did not communicate within 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.

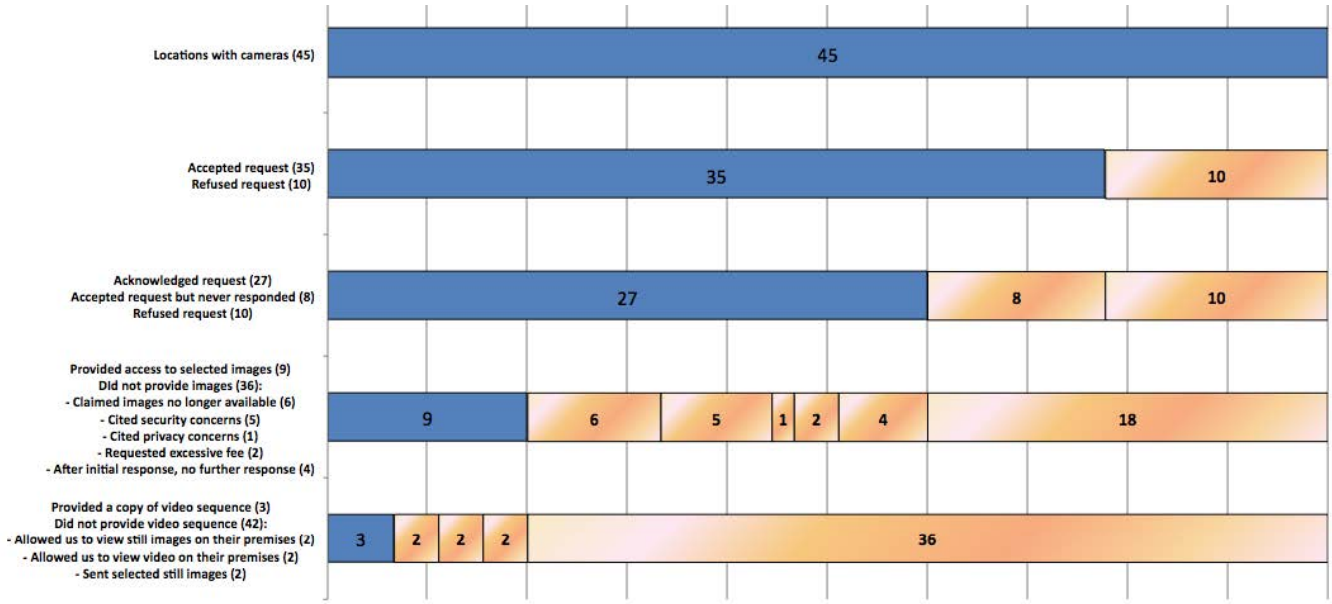

Fig 1: Outcomes of Requests for Personal Information, Phase I

Only 19 companies (13% of Phase I and Phase II combined), did so within the 30-day timeframe mandated by PIPEDA section 8(3). Figure 1 illustrates the outcomes of requests to obtain personal information for Phase I fieldwork (Phase II results were even more dismal.) It shows 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, 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.

4.5.3 Reasons for refusals to provide video

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.

4.5.3.1 Refused to provide video - citing security

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. Kanev had been standing in the parking lot outside a Beer Store outlet, photographing signage and video surveillance cameras 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". 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 little practical significance in terms of privacy.

4.5.3.2 Refused to provide video - citing privacy

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.

4.5.3.3 Refused to provide video - 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 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.

4.5.3.4 Refused to provide video - footage 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; correspondence from Le Chateau claimed "the video will erase in a week time". 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)

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 made the requests at the moment of video capture, the claim that footage has been deleted indicates that the processing of requests is uncoordinated and slow.

4.5.3.5 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.

4.5.4 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.

5. CONCLUSION

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 to 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. That intervention is now urgent. In this, the Canadian Privacy Commissioners and civil society organizations oriented to promoting civil liberties have important roles to play.

The next phase of this research will focus on enabling citizen action to hold video surveillance operators more accountable to privacy norms and laws.

6. ACKNOWLEDGMENTS

Our thanks to the Office of the Privacy Commissioner of Canada, which supported this research through a Contributions Program grant.

7. REFERENCES

[1] City of Toronto. 2008. Attraction Highlights. Retrieved from http://www.toronto.ca/attractions/attraction_highlights.htm

[2] Clement, A. and Ferenbok, J. in press. Mitigating Asymmetric Visibilities: Towards a signage code for (Canadian) surveillance camera networks. To appear in *Eyes Everywhere: The Global Growth of Camera Surveillance*, A. Doyle, R. Lippert and D. Lyon, Eds. Willan Publishing

[3] Directory of Major Malls, 30th ed. 2009. Suffern, N.Y.: MJJTM Publications Corporation.

[4] Deisman, W., Derby, P., Doyle, A., Leman-Langlois, S., Lippert, R., Lyon, D., Pridmore, J., Smith, E., Walby, K. and Whitson, J. 2009. A Report on Camera Surveillance in Canada - Parts One & Two. Surveillance Camera Awareness Network (SCAN). Queens University

[5] Federal Trade Commission. n.d. *Fair Information Practice Principles* Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[6] Ferenbok, J. and Clement, A. in press. Hidden Changes: from CCTV to "Smart" video surveillance. To appear in *Eyes Everywhere: The Global Growth of Camera Surveillance*, A. Doyle, R. Lippert and D. Lyon, Eds. Willan Publishing

[7] Gras, M. L. 2004. The Legal Regulation of CCTV In Europe. *Surveillance & Society*, 2, 216-229.

[8] Hier, S. P. 2010. *Panoptic Dreams: Streetscape Video Surveillance in Canada*. UBC Press.

[9] Lippert, R. 2009. Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality. *Social & Legal Studies*, 18, 505–522.

[10] Norris, C. and Armstrong, G. 1999. *The Maximum Surveillance Society: the Rise of CCTV*, Oxford, Berg.

[11] Office of the Privacy Commissioner of Canada (OPCC). 2009. Legal Information Related to PIPEDA. Retrieved from http://www.priv.gc.ca/leg_c/p_principle_e.cfm

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

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