'Smart' Private Eyes in Public Places?

Video Surveillance Analytics, New Privacy Threats and Protective Alternatives

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

Summary

This document reports on the research activities and findings for the 'Private Eyes' project, supported by the Office of the Privacy Commission through a Contributions Program grant.

We have:

- conducted three distinct phases of fieldwork studying private sector video surveillance practices in the Toronto area
- surveyed and summarized the literatures relating to the development of and research about video analytics
- developed a prototype of PIPEDA-compliant video surveillance signage
- disseminated the results of this research through a range of venues appropriate for engaging the varied constituencies relevant to private sector video surveillance.

Our main findings regarding video surveillance and signage practices in the private sector in the Greater Toronto Area (GTA), include:

- widespread adoption of video surveillance in leading private sector enterprises in their customer facing premises
- widespread non-compliance with PIPEDA openness and personal access requirements
- widespread ignorance of PIPEDA and its application to video surveillance
- video surveillance is largely handled by the security departments, leading to a "security over-ride" of privacy considerations.

Our main findings regarding Video Analytics include:

- much research and development work in being done in automated video analysis
- so far there is little to no sign of adoption of video analytic techniques so far in the GTA, but this could change quickly
- the topic of video analytics in retail sector is shrouded in secrecy, with a general reluctance among retailers and video surveillance operators to reveal their activities
- techniques for face/body detection and coding/blurring demonstrate promise for effective anonymization, but further development is needed.

We conclude that there is an urgent need for the OPC to help correct the current imbalance of the "security" approach of private sector firms over the privacy rights of individuals. This should include a combination of:

- audit video surveillance practices in the private sector
- educate the public around video surveillance and privacy rights
- enforce PIPEDA more strongly in relation to video surveillance
- publicize the more egregious privacy violations of video surveillance operators
- promote de-identification techniques in video surveillance systems
- improve the signage requirements for video surveillance installations

Table of Contents

Appendices

0 Introduction

The deployment of video surveillance systems in Canada has been increasing since the 1990's. The growth has been particularly noticeable in the number of cameras we can see on the streets and in shopping areas. Much of this surveillance appears not to be compliant with PIPEDA, at least judging by the relative lack of signage. Less visibly, but no less importantly in the long term, is the development of supporting digital techniques for image capture, storage, networking, and, perhaps most significantly, algorithmic processing.

The goal of this project is to make video surveillance operations and algorithmic techniques more transparent and publically accountable, by gathering information on the technology and industry practices and educating the public about the field and its privacy implications. This project looked at video surveillance installations, research, policy and applications as they are relevant to Canadian private sector settings where personal information may be captured.

The project has pursued this overall goal mainly through four broad activity areas:

1. Conducting a three phase field study of private sector video surveillance and signage practices in the Greater Toronto Area;
2. Surveying the state of the art of video analytics;
3. Developing a PIPEDA-compliant video surveillance signage scheme;
4. Reporting the results of the research in a variety of public venues.

These are each discussed in the following sections.

1 Video Surveillance and Signage in the Greater Toronto Area

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 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 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 an individual expect in terms of the collection of their personal information? If an individual attempts to exercise her rights under PIPEDA, will her right to request and access that information be respected?

We conducted the fieldwork in three phases, each with similar but distinct aims and methods. The first phase targeted industry leaders in video surveillance deployment (45 locations), the second targeted two major shopping malls and all the retail stores within them (258 locations). The third phase, still in progress, targeted surveillance cameras overlooking public spaces (40+ locations). By the nature of the samples, cameras were found in all the locations in the phase one and three, while in phase two, cameras were found in 40% of locations.

Signage for video surveillance operations was generally absent. 65% of the phase one locations with cameras had no signage while in the phase two sample 73% were without notification. Where there was signage, it was often lacking in placement, visibility and required content (eg, purpose, contact information) and worded vaguely, ambiguously and in some cases actually misleading. We did not observe a single sign that we judged as meeting PIPEDA requirements. (This has led the principal investigator to offer a $100 reward for spotting the first PIPEDA compliant sign for a private sector video surveillance operation.)

In questions posed to store managers about the handling of personal information in relation to the video surveillance and the processing of writing requests to obtain access to personal information in the video recording, a similar pattern of weak to non-existent PIPEDA compliance was revealed. Indeed, in some cases requests for information were treated with hostility, reflecting an apparent preemption of personal privacy rights by the security interests of the organization.

This fieldwork presents a disturbing picture of a serious imbalance in the relations between individual citizens/customers and surveillant organizations, with individual rights clearly subordinated in all but a few cases. This situation poses a potentially grave challenge to the authority and effectiveness of the privacy regulator, which left un-remedied will lead to the widespread and long term erosion of privacy protection in the private sector.

For further details, see Appendix A: Fieldwork Report on Video Surveillance and Signage in the Greater Toronto Area.

2 Video Analytics

The second major branch of this research project examined the growth and privacy implications of automated analytic techniques within video surveillance operations. Although scattered across

many disciplines and known by many terms, the automated extraction of metadata from video images, what we refer to as Video Analytics (VA), is an active research area and a developing technological edge in surveillance and measurements of consumer behaviour. It is also clear that large stakeholders like Sony, Intel and Bosch are already trying to deploy 'intelligent' video surveillance systems particularly for large scale zone surveillance, traffic monitoring and for consumer metrics (see Bosch and CognoVision discussions). The features of these advertised systems go well beyond people counting to a range of analytic measures of an individual, event, behaviour etc. Though they do not appear currently to promise ubiquitous tracking across multiple zones and cameras, or one-to-many identification at a distance, it is clear that the sophistication of the techniques and technologies is improving. It is also clear that these algorithms are only the first round of video analytic strategies, applications and granularity. What remains unclear is the success of deployment or the actual effectiveness of these systems to perform as promised. As of yet, there is little evidence that these systems are being actively deployed in the GTA by retailers in publically accessible spaces.

Based on observations and field work it appears that the retail surveillance in publically accessible spaces has hardware that lags behind current generations of consumer electronics. Camera side analytics will likely remain bound to event detection and recognition applications like traffic monitoring until higher resolution digital video cameras are deployed. This will likely change in the near future. As cameras are updated video analytics and digital signal processing incorporated into cameras may become the norm.

The fact that currently installed video cameras are not suitable for VA, does not necessarily mean that digital signs, with their own dedicated cameras are not being employed. These cameras tend to be much smaller than conventional surveillance cameras and hidden behind screens or point-of-purchase signage. Consequently these cameras and associated networks are much harder to spot and present a more difficult privacy issue to tackle as they often claim they do not record video information but only gather marketing data such as gender and age—privacy protected information—along with a host of other marketing metrics. While it is clear that deployment of VA or digital signage in the GTA is limited at the moment, the fact that suppliers are now advertising 'intelligent' video surveillance among core product offerings, that at least one retailer has confirmed that they have rudimentary analytics installed, that anecdotally we know businesses are investigating these technologies, that software systems represent only a relatively small incremental cost where camera infrastructures already exist, and that companies like Facebook are already compiling data-bases for face-recognition, it would seem likely that this scenario will change in the short term. It behooves privacy advocates, in anticipation of pending wider deployments, to learn more about how these systems capture, process and distribute information to understand how individuals will be affected by these new ‘smart’ and unwavering private eyes.

One area where these video analytic capabilities can be used for privacy protective purposes is in the de-identification of video surveillance images. Research at the University of Toronto has developed a “Secure Object Level Encoding” technique that is well suited to encrypting people’s faces or entire bodies so they cannot be viewed and identified without authorization to do so. As

part of this research we tested a prototype of this software being developed commercially with Xiris Automation. We evaluated capabilities by applying it to video surveillance footage we had obtained through personal information requests in the early fieldwork stage of the project. We also successfully demonstrated with an in situ de-identification of the audience at the IPSI Research Day that we convened in part for this purpose. Overall, when deployed in a privacy sensitive framework face de-identification as a privacy enhancing strategy will likely prevent unauthorized access without compromising security. Once the viability of this technique is established, then by the data minimization principle those that do not incorporate this feature will be non-compliant, and potentially forced to adopt de-identification as the standard.

For further details, see Appendix B: Report on Video Analytics in the Greater Toronto Area.

3. PIPEDA-compliant video surveillance signage scheme

The third major branch of this research project was to develop a signage scheme that could address the principal shortcomings of existing video surveillance signage. The main findings of our video surveillance fieldwork reported above concerning signage are that the great majority of video surveillance installations (60-70%) have no signage whatsoever, and that where signage is present, it does not comply with PIPEDA. Signs tend to small, hard to read and placed in obscure locations—limiting their effectiveness as mechanism of informed consent. Signs vary considerably in visual appearance and in their wording, failing to inform customers without undue effort of the scope, nature, purposes and uses of the surveillance systems. This non-compliance appears to stem from at least three related issues: an ignorance of what is required for compliance, a lack of clear exemplars of good practices for surveillance signage and the absence of effective regulatory enforcement. While the various Privacy Commissions do provide some important guidance on what signs should contain, they do not address all the aspects of a video surveillance operation that a citizen may reasonably seek to know in order to make an informed decision about whether or not to enter a surveilled space and how to behave within it, such as whether there is live monitoring, whether images are stored and for how long. Furthermore, the guidelines don't take into account the possibility that various forms of video analytics may be used to process images of the individual in making potentially consequential inferences about the person.

To help remedy these shortcomings, we have developed a signage scheme that can serve as a starting point for formulating a signage standard suitable for widespread adoption. Our signage takes as a foundational premise that people need to be sufficiently informed before they walk into a surveilled space about its main characteristics to determine whether to proceed or take another route. Inspired by highway traffic signage conventions, in terms of colour, font, layout, iconography, which are similarly designed to convey complex information in a timely manner, we developed iteratively a series of prototypes for video surveillance signage (See Figure 1).

For further details, see Appendix C: Mitigating Asymmetric Visibilities: Towards a Signage Code for Surveillance Camera Networks.

Figure 1: Prototypes of PIPEDA-compliant video surveillance signage

We have discussed with several potential partners we encountered in the first phase of our fieldwork the possibility of a retail trial of the compliant signage. However, to date no enterprise has agreed to try it out and we have been able only to gather anecdotal evidence regarding the reception and effectiveness of any potential scheme. This lack of response appears likely related to the reluctance of any organization to break with the prevailing retail industry norms, which prefer keeping a low profile and avoid alerting customers to their surveillance activities, over being a visible leader in PIPEDA compliance. It appears likely that this will not change until there is much more pressure on surveillant organizations to take privacy seriously in their video surveillance operations. In the meantime, we intend to continue looking for partners willing to work us in customizing our prototypes in response to field testing.

4. Public dissemination

Given the widespread ignorance of the privacy dimensions of video surveillance, on the part of both private sector video surveillance operators as well as the public more generally, an important aspect of this project has been to reach the various relevant parties with the results of our research and engage them in reforming video surveillance practices.

We made two presentations to privacy professionals:

> Private Eyes in Public Places? Toward a (Canadian) video surveillance signage code, presentation to the Privacy Professionals' Community of Practice, Oct 1, 2010
>
> Private Eyes in Public Places: Signage and PIPEDA (Non) Compliance, presentation to the International Association for Privacy Professionals (IAPP) Conference, Toronto, May 6, 2011. (See Appendix E)

We convened a public research forum on video surveillance (and privacy protective digital ID) at the University of Toronto:

> Private Eyes Video Surveillance, presentation at Identity Privacy and Security Institute (IPSI) Research Day, University of Toronto, June 20, 2011. (See Appendix F)

In conjunction with the fieldwork, we created the Canadian Surveillance Camera (aka CCTV) Signage Flickr Group (See: http://www.flickr.com/groups/1233129@N25/) for publically sharing photos of surveillance cameras and signs. This group currently has 32 members and 648 photos, mainly in the Toronto Area.

We led two well-attended public "(Video) Eyes on the Street" Jane's Walks in Toronto, one on May 8, as part of the international weekend of Jane's Walks (see: http://www.janeswalk.net/), and the other on May 15, one of three public events held in conjunction with the Cyber-Surveillance in Everyday Life research workshop, part of the New Transparency project. (see: http://www.digitallymediatedsurveillance.ca/). These walks are documented in the video *(Video) Eyes on the Street - A 2011 Jane's Walk,* available on YouTube (see: http://www.youtube.com/watch?v=VCzH2mpGYxE).

All these materials are publically available on the project website: http://surveillancerights.ca This report will also be posted to this site.

5. Conclusion

This research has revealed a stark and clear picture of contemporary private sector video surveillance operations, at least in the heavily trafficked shopping areas of Toronto. 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 living in urban areas who wish to participate fully in society have no choice but to be under near-constant surveillance when in public and commercial spaces, 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. A security worldview appears to pervade video surveillance operations, and typically this 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. Anyone asking questions, even simply about how their own information is being handled, risks being treated as suspicious and threatening. While there can be legitimate security concerns that call for video surveillance measures, these need to be demonstrably necessary, effective, proportionate, minimally intrusive to law abiding citizens and compliant with legal requirements regarding personal privacy.

The lack of knowledge of basic PIPEDA requirements among front-line retail managers and the apparent lack of privacy oversight within many retail organizations clearly contribute to this situation.

Another contributing factor is the lack of public awareness and involvement around video surveillance matters. There are few sources of readily available information about the privacy dimensions of video surveillance, and those few customers who seek to find out what a surveillant organization is doing with their video images, or otherwise exercise their privacy rights, are likely to find the process frustrating and may even encounter outright hostility. This dynamic breeds 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 make their activities more visible. As long as the leading companies maintain a consistently low profile, few citizens will even know how to enquire or 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.

In remedying this imbalanced situation in favour of the citizen and consumer, the OPC obviously has a leading role to play. To start, it 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.

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.

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

The growth of video analytics threatens to worsen the situation, especially if there is no strengthening of the notification requirements to alert consumers of automated video processing and classification when it does occur. Fortunately there appears to be at least a short period of time before video analytics becomes widespread in the private sector. To take advantage of this window of opportunity, the OPC should consider investigating the potential risks and remedies, and helping educate the public understand the implications. It can also promote the use of video analytics for privacy protective purposes, such as the routine de-identification of video surveillance signals, with decryption only with proper authority and supervision in cases that actually call for identification.

Finally the OPC should consider re-visiting its guidelines for video surveillance, revising them in light of the experience with them to date and in light of the impending spread of video analytics. In particular, it should improve the signage requirements to include appropriate notification of live viewing, recording and use of various video analytic applications.

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.

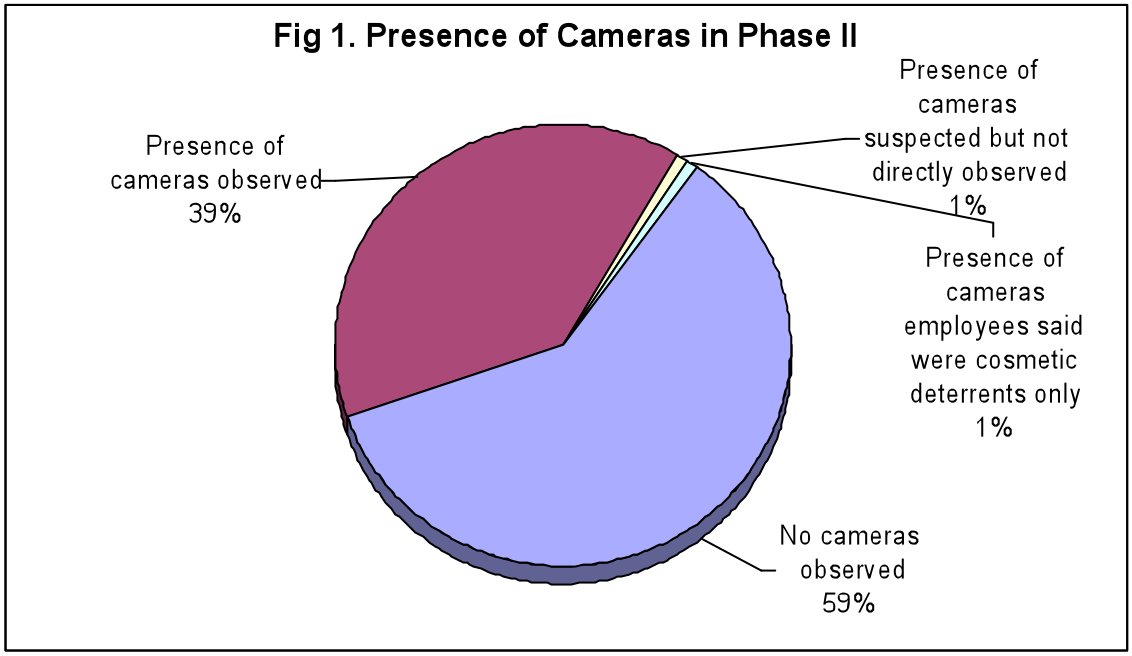
Of the 101 locations where video cameras were observed (this includes the two locations were employees told researchers the cameras were fake), 32 locations (32%) had video cameras on the exterior of the storefront. Of those 32 locations, researchers judged that in 23 locations (71%), cameras were likely 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

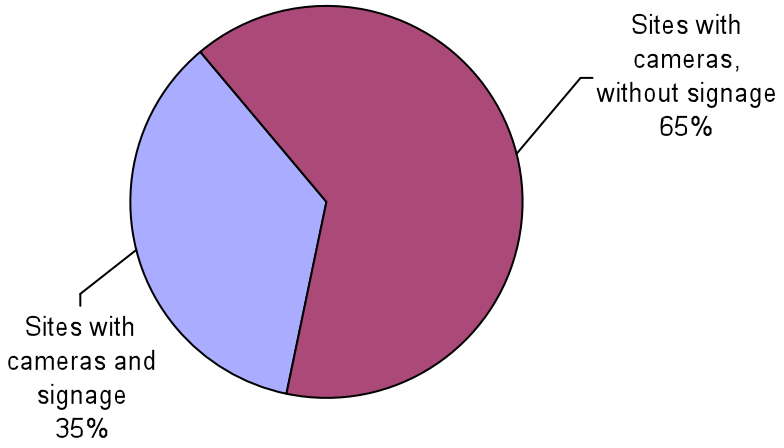
questions. However, as Clement and Ferenbok (2011) observe, the explicit notification requirements are found in guidelines that are meant to assist companies "with the deployment of their video surveillance systems and are not binding or enforceable" (p. 5). That is, the notification requirements enable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

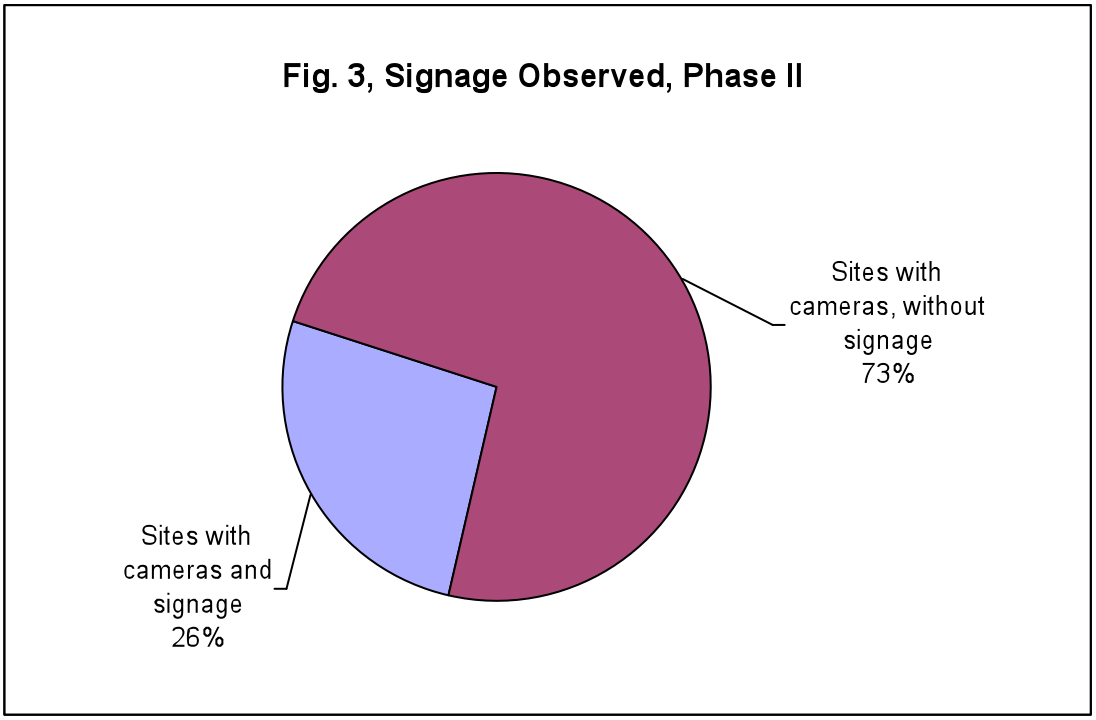
Fieldwork data clearly illustrates both the lack of signage generally and the lack of PIPEDA-compliant notification among private sector organizations with a consumer point-of-contact. As shown in Fig. 2 below, of the 45 locations sampled in Phase I, all of which used video surveillance, only 16 locations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

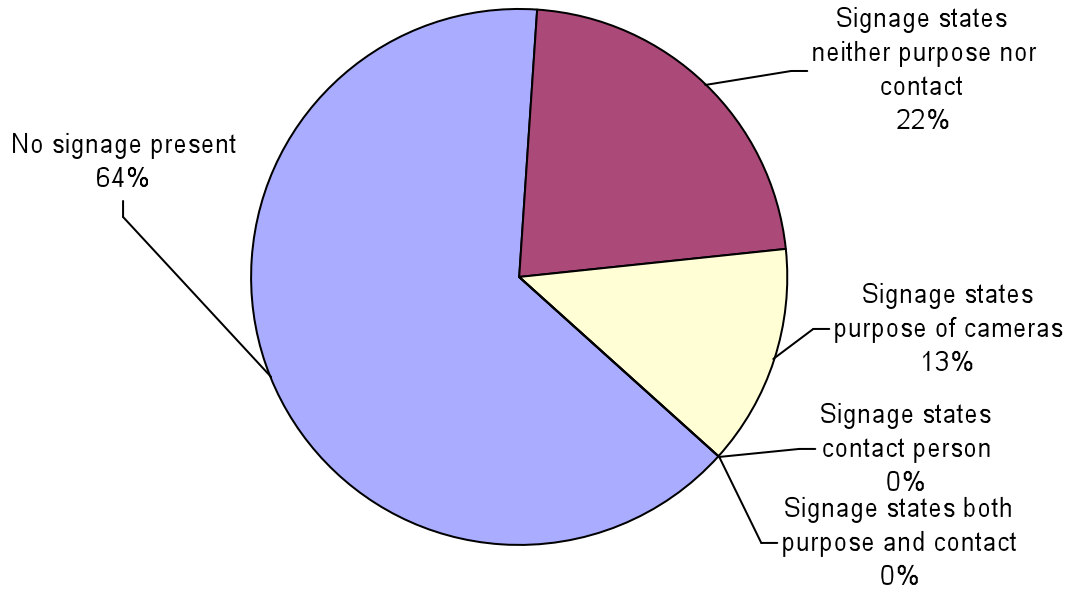
> The information made available shall include:
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and

> 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.

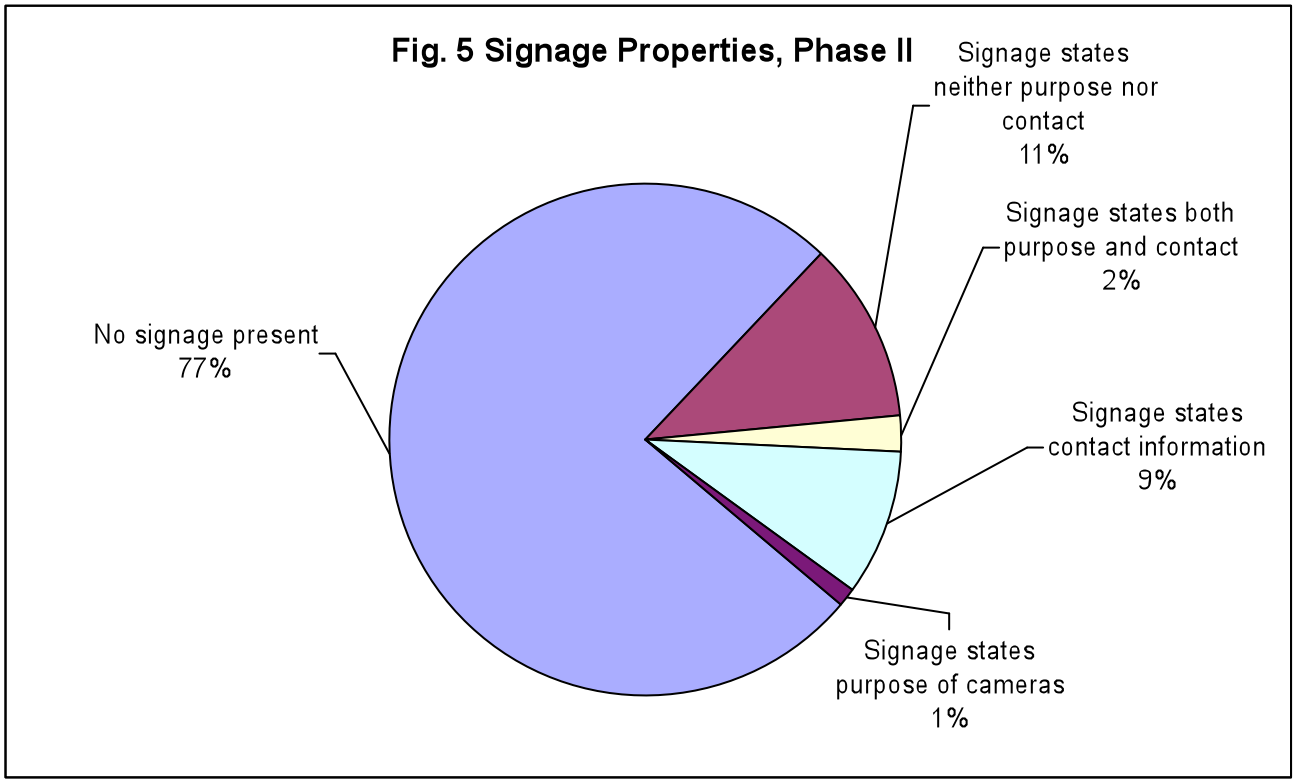
Fig. 4 illustrates several key properties of the signage observed on the premises of the organizations sampled in Phase I. Only 16 out of 45 (35%) organizations in the Phase I sample used any signage notifying the public of the presence of video surveillance. Of the 16 signs observed, most contained 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

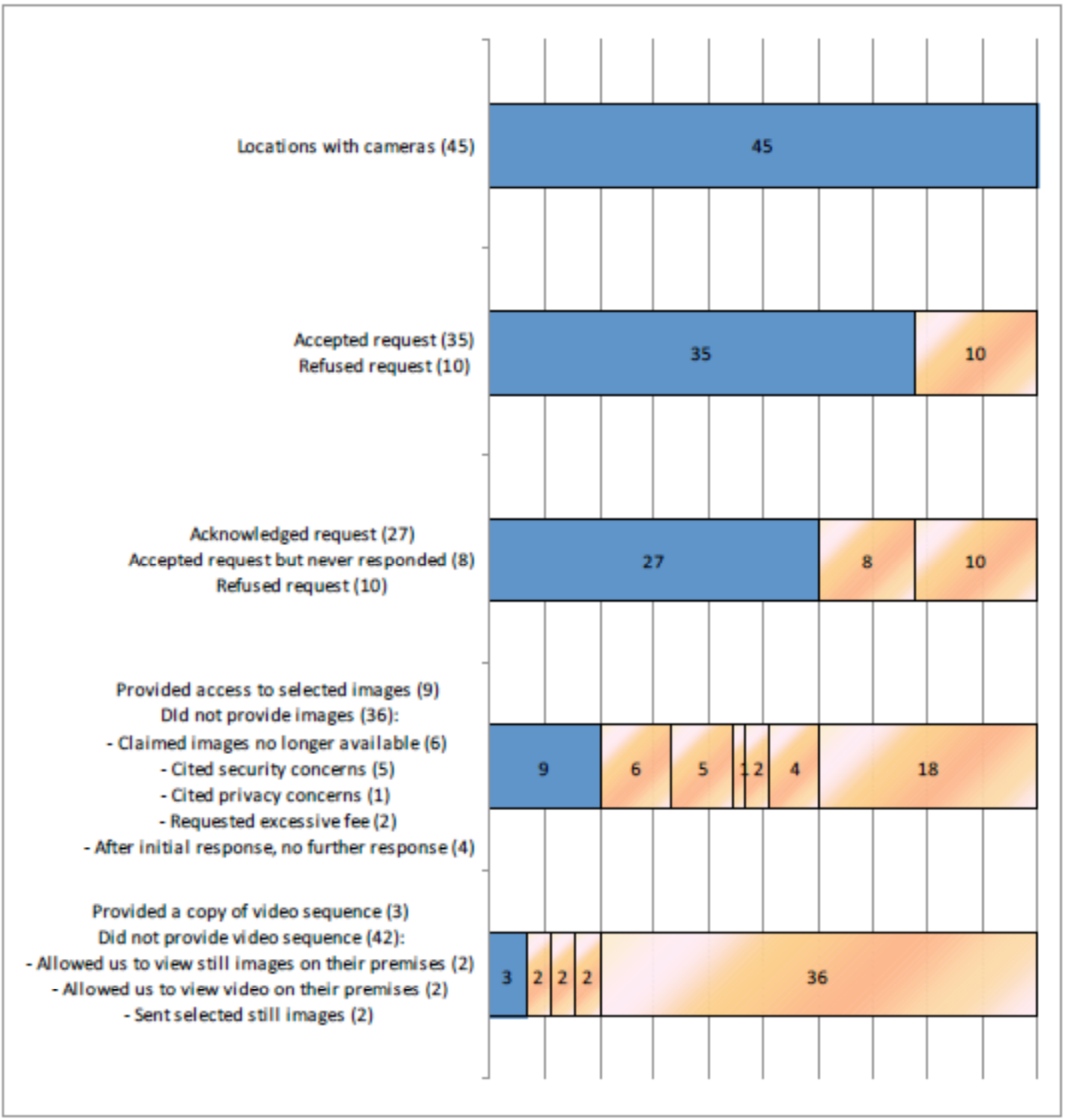
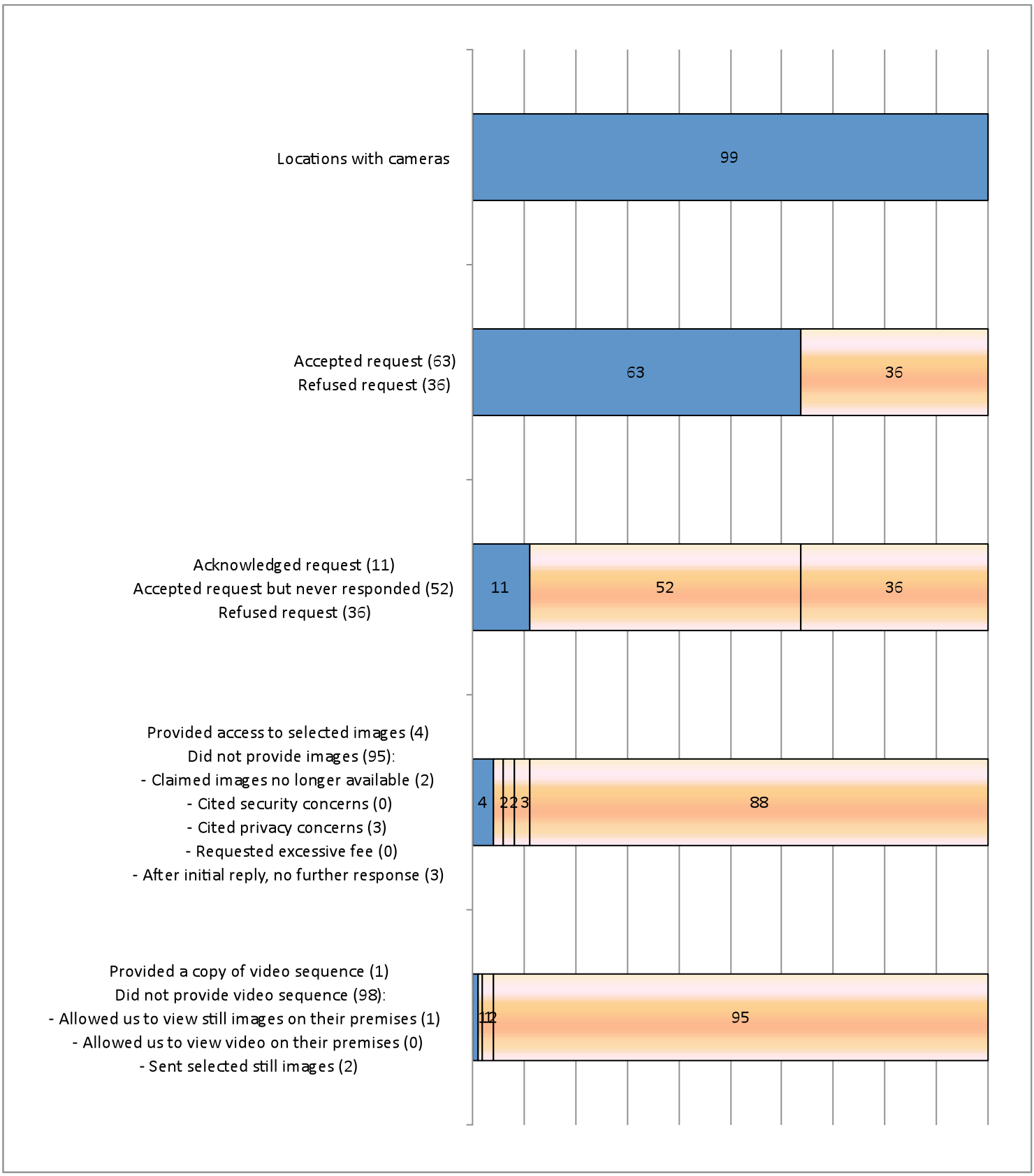


Fig 7. Outcomes of Request for Personal Information, Phase II



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: Signage

Appendix B, Fig. 1. Signage on entrance to Toronto Eaton Centre

Fig 1a. Close-up of sign

Text of sign: “As Part of Our Management Services Cadillac Fairview Uses Closed Circuit TV at This Property”

Fig 1b. Sign in context of entrance

Sign is at top of glass door.

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

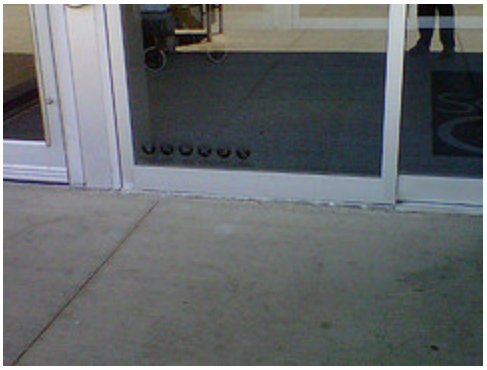


Fig. 2c. Sign in context of entrance

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

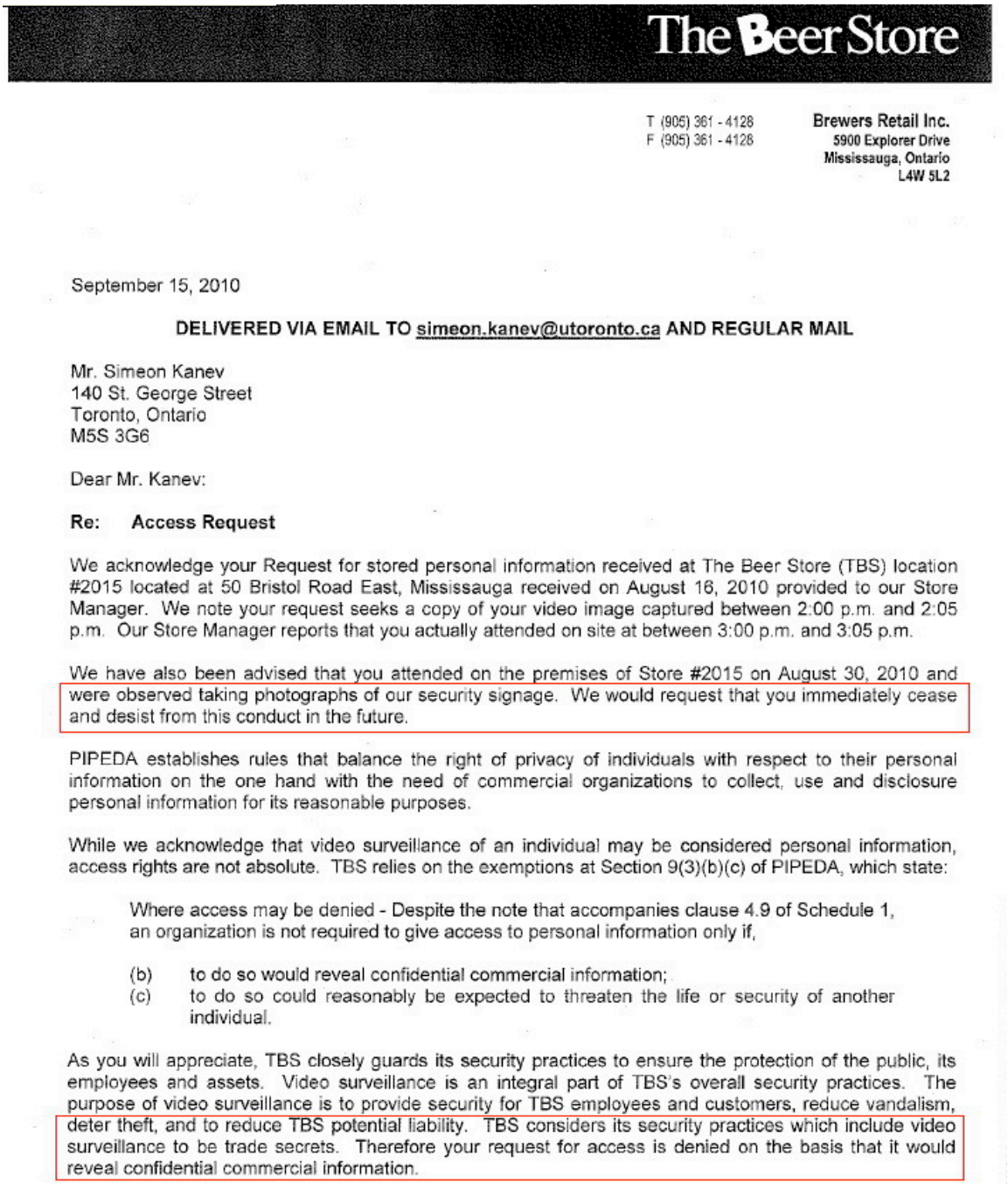
Text of sign: Property Protected By / DIGITAL VIDEO SUREVEILLANCE / From/ Checkpoint Canada Inc. / [company phone number and website]

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.

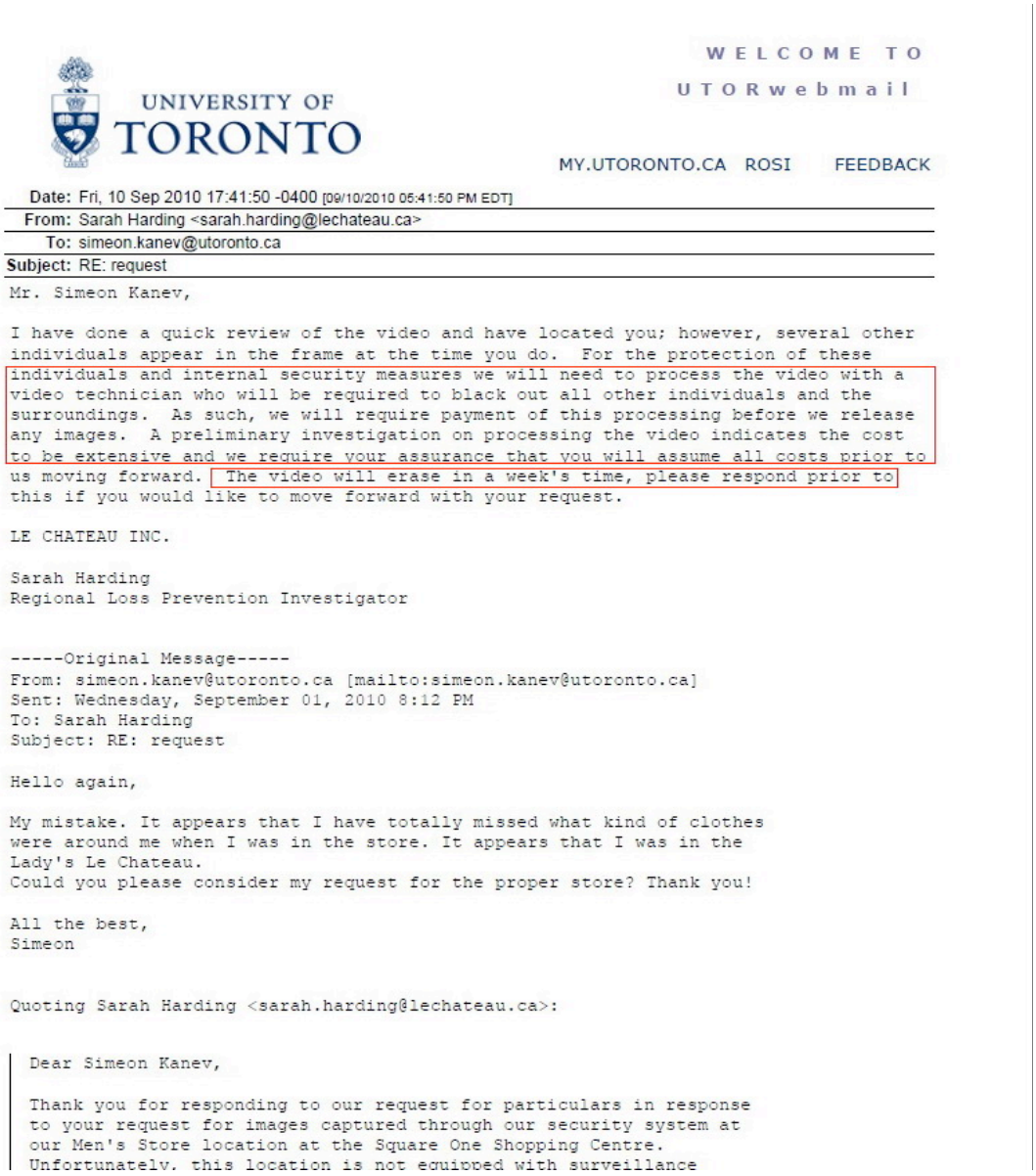
Given the above, your access request is denied in accordance with the provisions of S. 9(3)(b)(c) of PIPEDA.

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

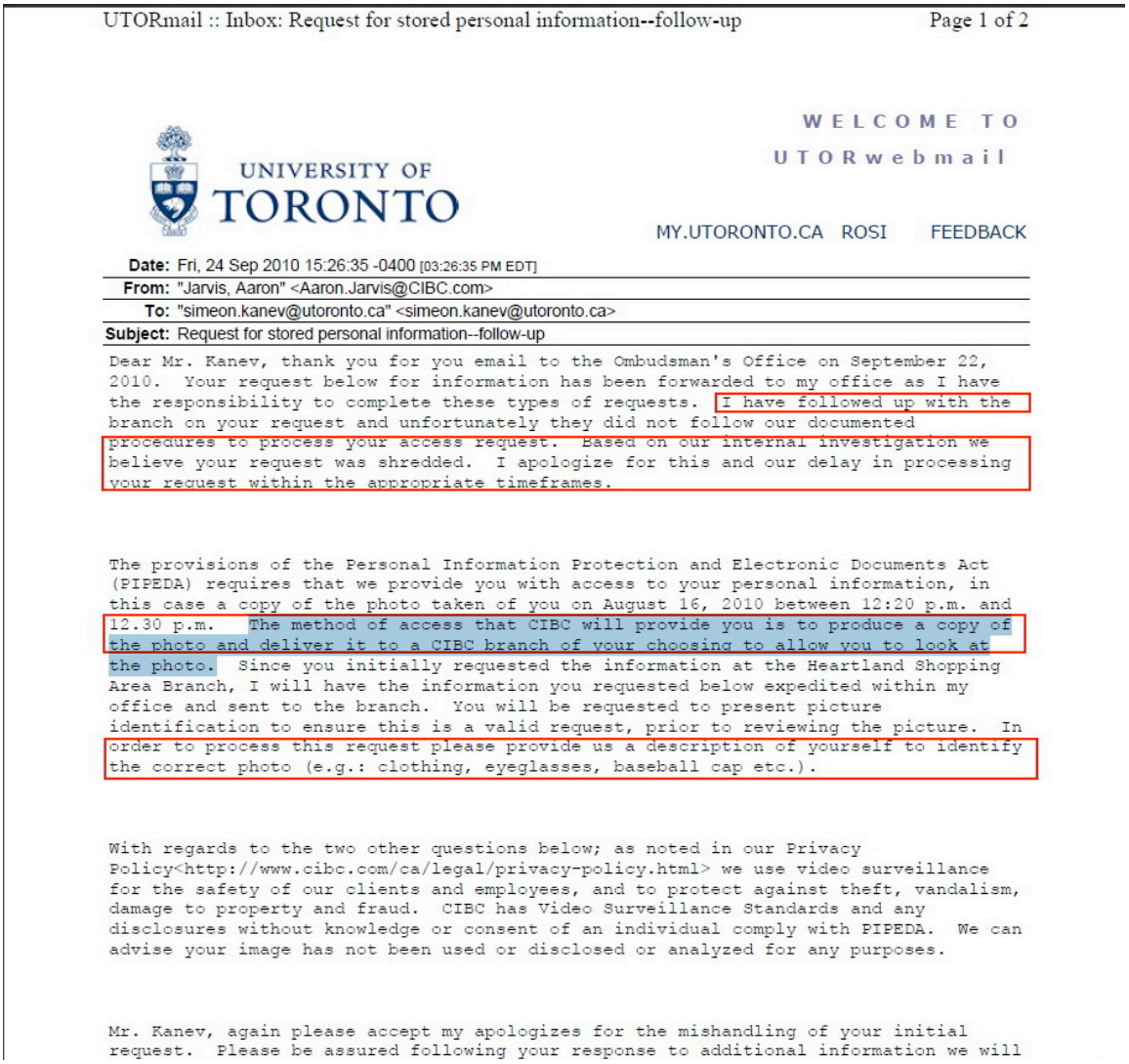
From: Bryna Berman [wma.bryna@gmail.com]
Sent: Tuesday, June 21, 2011 9:36 AM
To: video.privacy.issues@gmail.com
Subject: Wm. Ashley

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

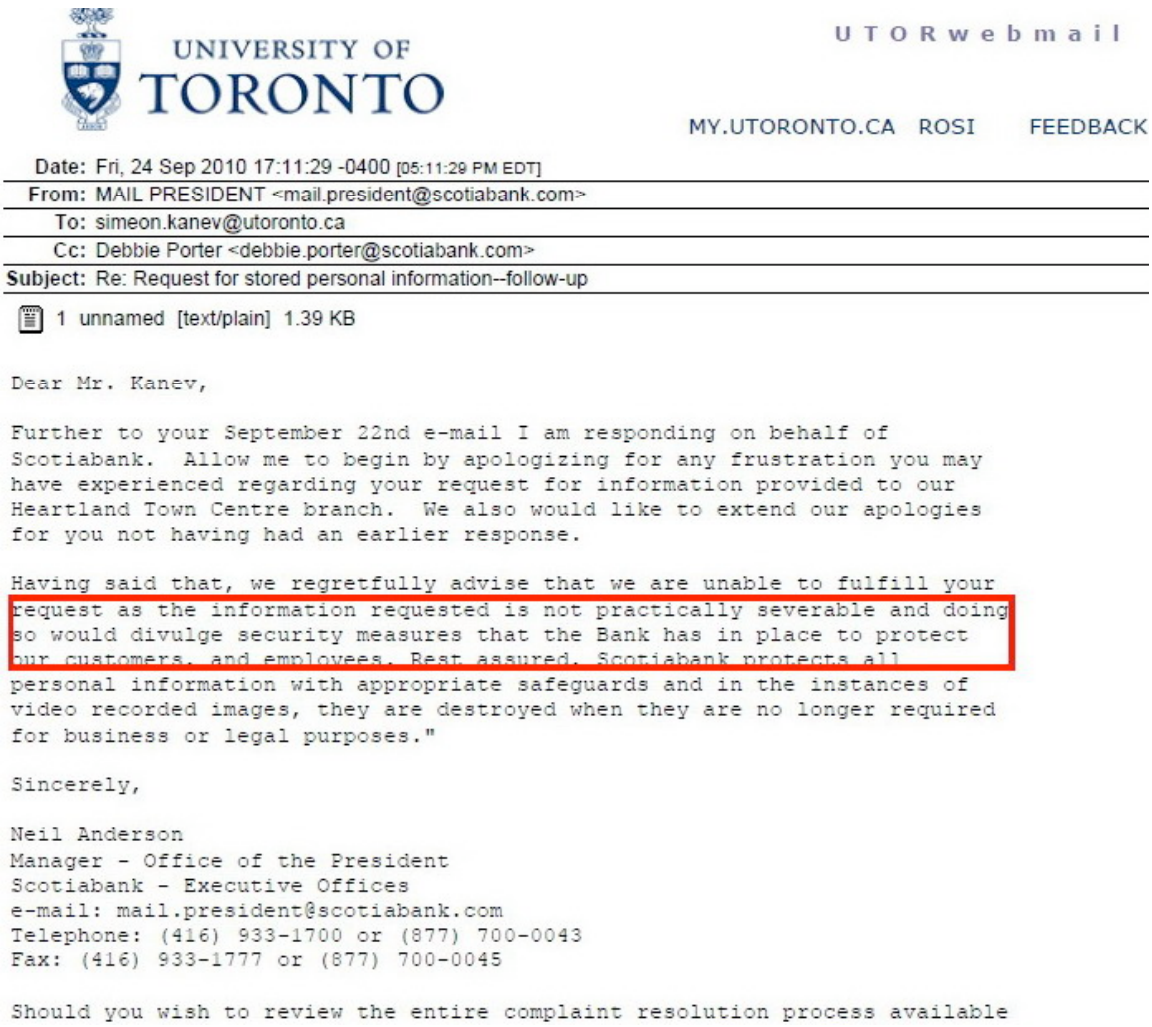
Dear Mr. Kanev, thank you for you email to the Ombudsman's Office on September 22, 2010. Your request below for information has been forwarded to my office as I have the responsibility to complete these types of requests. I have followed up with the branch on your request and unfortunately they did not 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

Appendix B

Report on Video Analytics 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	Joseph Ferenbok & Silvia Valdman
	Information Policy Research Program, Faculty of Information, University of Toronto
Corresponding Author	joseph.ferenbok@utoronto.ca
Date	23 July 2011

Table of Contents

1. Purpose

The purpose of this report is to outline the literature, technologies and practise of the growing area of what is labelled here as video analytics—or the automated processing of video to derive 'meaningful' information. The literature gives a broad perspective on video analytics (VA) while the survey of technologies and practises was conducted mainly throughout the Greater Toronoto Area (GTA). We also specifically evaluate the Xiris video analytic system for de-identifying faces.

2. Introduction & overview

Increasingly, video surveillance systems integrate one or more layers of algorithmic analytics that mediate the flow of information between the operator(s) and the camera(s). This intermediate video processing, which may start at the camera but continue long after information has been recorded and stored, is referred to here as Video Analytics (VA). Although vendors also use terms such as smart video surveillance, Intelligent Video Analytics (IVA), Intelligent Analytics (IA), Video Content Analysis (VCA) to describe a range of video image processing techniques the term video Analytics will be used here to incorporate a range of functionality “from systems that classify and store simple data, through more complex systems that compare the captured data to other data and provide matches, to systems that attempt to predict events based on the captured data” (Norris and McCahill, 2006). Video Analytics as a form of digital signal processing allows for algorithmic surveillance (Introna and Wood, 2004) that is hidden from even the most observant surveillance subject.

What is video analytics?

Conventional, analogue CCTV cameras were limited by the required balance between the volume of information multiple networked cameras generated and the amount of resources necessary to screen, store and analyze the visual data. The deployment of digital video surveillance through Internet Protocol (IP) networks have and continue to change the balance between captured information and our ability to analyze and interpret data. Video Analytics is the umbrella term used to include a range or assemblage of technologies that convert visual data into information for purposes of automated surveillance (Gorodnichy, 2010).

Video Analytics rely on a foundation of hardware infrastructures. Analogue surveillance systems may still be found but increasingly suppliers are selling

digital equipment with increasingly more sensitive sensors, increasingly higher storage capacities and cheaper operating costs. It is not surprising that the retail sector is using digital cameras and storage for store level surveillance. Once infrastructures are in place however, it becomes difficult to assess how that information is processed. Video Analytics is conceptualized here as the software layer that turns the collection of digital video into meaningful information for automated decision making.

Understanding video analytics as software however is still itself a major task because programming computers to detect, classify, code and semantically label temporal and spatial patterns of pixels in a video stream is a complex problem. Video Analytic software involves a series of tasks that help computers to visually 'understand' contextual events like objects moving to a pedestrian falling. Video Analytic software or smart computer vision has a range of applications from ensuring proper welds in factories to detecting forest fires, to tracking customer patterns and identities.

Perhaps because of the complexity and scope of 'teaching' machines to see, video analytic architectures tend to be modular -- that is a series of software modules strung together -- where outputs of one module are used as inputs for the next. Generally an early processing stage includes a module that attempts to distinguish and track objects across successive video images. Differences between frames can help demarcate moving objects in the foreground from the background. Once detected, the background is subtracted, or discarded, so subsequent object and event detection modules can process the pixels that remain, for instance by comparing them with patterns in earlier frames or pre-defined reference models.

The image information can then pass on to object and event classification modules where patterns are classified and alerts triggered automatically. The criteria for alerts are based on predefined or user-specified models for various types of objects and events, such as the presence of a gun, a person running or an unexpected package. In the classification stages video analytic engines produce meta-data that both guides the visual processing and provides semantic descriptions of the video inputs. This classification of objects and events can also produce an index of objects and recognized events, which in turn can be used as meta-data for future search and retrieval and as data for further processing.

Based on the semantic coding of object recognized—e.g. a vehicle, body, or face—other algorithms may be employed to identify objects individually and track them between frames and across different video streams. If an object is classified as a license plate, for example, automatic number plate recognition (ANPR) (also known as automatic license plate recognition (ALPR)) software can then be used to correct any distortion and apply optical character recognition (OCR) to identify the registration.

An object determined to be a body can be analyzed for individual identity or behavioural pattern (e.g. 'loitering'). Though perhaps further off than ALPR in terms of routine adoption, but at least as challenging with respect to policy and individual rights, are the analytic techniques for behavioural analysis and biometrics such as gait or face recognition. Tracking and identifying people in

video is an active area of research, development and commercialization (Cai et al., 2009, Bojkovic and Samcovic, 2006, Gorodnichy, 2006, Shaokang et al., 2008, Suman, 2008, Goffredo et al., 2008).

II. Technologies and practices in GTA

The surveillance industry is a complex network where multiple actors shape the landscape the overall industry. Among these stakeholders are those who provide video surveillance services and equipment across the Greater Toronto Area (GTA). These include: retailers, commercial services (suppliers and consumers), wholesalers, manufacterers, and software developers.

Four site visits to venders of video surveillance equipment in the GTA suggests that currently few are carrying products augmented by 'video analytics'. When the concept of automated surveillance was discussed, retailers inevitably turned to products that included software for managing one or more surveillance cameras in a network. Two software suites were reviewed by the researcher that are packaged with wireless IP cameras (one Cisco, one Sony) and in both packages the software included options like remote IP video viewing, automatic 'patrol' and motion detection, but more suffisticated algorithmic analytics were included. Part of the issue seems to be that many of the cameras on sale are still measured in TV lines (400 — 540 TV lines is currently still a typcial range). This resolution provides only very coarse grain information and makes object recognition, event detection, human detection and identification, more difficult—garbage in, garbage out. Although HD cameras are available (1.3 megapixles or more) they are still relatively expensive and feature-poor.

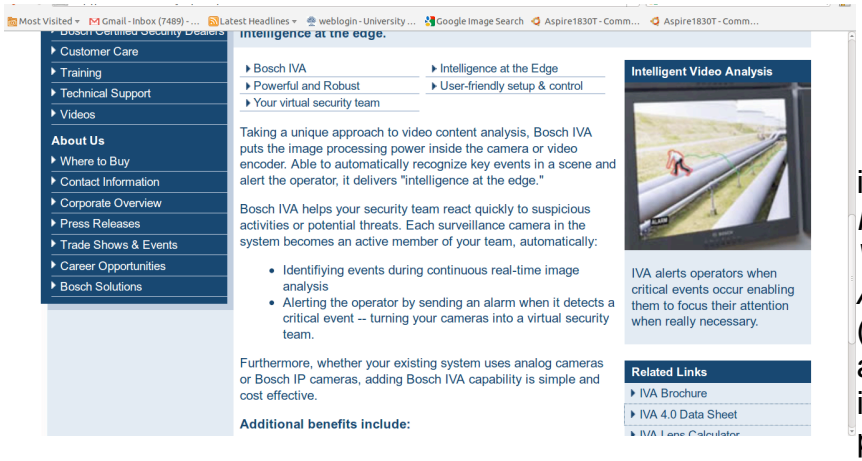
In our field work of retailers who employ video surveillance, only one retailer openly divulged that they employ automated people counters as part of their video surveillance—the Apple Store. But the employee also hat their video surveillance is networked and has remote access capabilities. So the infrastructure for harvesting video analytic information is already in place. It is only an incremental step to include software on the backend of an existing system—one that can remain entirely hidden.

A review of suppliers of commercially available video surveillance services suggests again that video analytics is still only at the very cusp of deployment. Security Companies in the GTA were unresponsive to requests to discuss video analytic technologies. During one site visit, the Director of Loss Prevention said “I not currently intersted in video analytics. I looked at it a while back but I can't see any advantages at the moment. But I think that [competitor X] is looking into it for their stores”. A site visit to one of this competitor's store suggested that none of the front-line security personnel were aware of any automated system used by the retailer. A subsequent information request initated by the researcher and the research assistant did not suggest that the retailer has any analytic capabilities.

Video Analytics vendors

Bosch

Looking at the manufacturers of surveillance cameras tells a different story. Bosch, a leading supplier of video surveillance equipment in North America,



includes *Intellent Video Analysis* (IVA) along side its core product offerings.

Bosch is directly claming that Intelligent Video Analysis can help augment human performance—addressing an established problem with human monitoring: attention span. The company claims that their system can recognize perimeter breaches and atypical behavours to bring to the foreground cameras where incidents may be occuring.

Bosch states that “no matter how few or how many cameras your system uses” their Intelligent Video Analysis can help you use your resources more efficiently. In Bosch's system the IVA is performed on a chip in the camera itself rather than

at a centralized monitoring station. The embedded digital signal-processing allows for objects to be recognized and coded in a meta-data stream (see figure 2) that may then be used to trigger events and process or aggregate data. The 'meta-data' stream can be decoupled from the original video for further processing, aggregation, modelling and other forms of 'intelligent' viewing.

Bosch lists among the advantages of this system, cameras with on-board digital signal-processing, that you don't need analysis servers or operating systems; and no need for centralized hardware.

Cognovision

Cognovision, now a part of Intel, is another piece of the future of Video Analytics. Instead of augmenting human performance, they measure it. CognoVision's core competencies centred around audience 'measurement' and & retail intelligence. According to their website, “CognoVision helps retailers & digital signage networks measure the effectiveness of in-store marketing and

understand shopper behaviour" (retrieved July 20, 2011) .

Amongst CognoVision's focus is retail intelligence by monitoring and classifying different levels of customer engagement. The company measures dwell time and traffic flow all with the promise to increase business—ultimately sales. Dixon (2010) has discussed how some large American retailers already employs such customer surveillance techniques in their stores. This trajectory seems to beg the question as to what degree is a corporation's ability to profit from an individuals personal information habits, before that corporation is breaching the right to information self determination.

Summary

The retail and security video surveillance market appears to be lagging behind the consumer imaging technologies like laptops and cellphones. Video surveillance vendors sell High Definition cameras of 1.3 megapixels or more, but these are relatively new and generally cost prohibative for small business or mass deployment. Surveillance camera retailers still discuss resolution interms of TV lines (400 — 540 is typical), while 1.3 mpx webcams (more than three times the resolution of 540TV lines[1]) are typical on most laptops and netbook computers.

Companies are currently offering systems that are supplementing traditional CCTV practices with video analytic features. Whether called Intelligent Video Analysis or Video Analytics, these products are already being offered. As the cost of sensors comes down, and higher resolution networked cameras become typical, adding video-analytics software becomes an incremental cost

1 Assuming a 3:4 aspect ration.

that may offer more granular and meaningful information. As video information captured in publically accessible spaces becomes more common and valuable, these issues of an individual's right to information self-determination will undoubtedly become more prevelant.

Video Analytics (VA), is an active research area and a developing technological edge in surveillance and consumer metrics. It is also clear that large stakeholders like Sony, Intel and Bosch are already trying to deploy 'intelligent' video surveillance systems particularly for large scale zone surveillance, traffic monitoring and for consumer metrics (see Bosch and CognoVision discussions). The features of these advertised systems go well beyond people counting to a range of analytic measures of an individual, event, behaviour etc.,. Though they do not seem to currently promise ubiquitous tracking across multiple zones and cameras or one to many identification at a distance it is clear that the sophistication of the techniques and technologies is improving. It is also clear that these algorithms are only the first barrage of video analytic strategies, applications and granularity. What remains unclear is the success of deployment or the actual effectiveness of these systems to perform as promised. As of yet, there is little evidence that these systems are being actively deployed in the GTA by retailers in publically accessible spaces.

Based on observations and field work it appears that the retail surveillance in publically accessible spaces has hardware that lags behind current generations of consumer electronics. In the GTA video equipment suppliers are still selling equipment that measures image quality in TV lines rather than Megapixels. Camera side analytics will likely remain bound to event detection and recognition applications like traffic monitoring and perimeter security, until equipment is upgraded to include higher resolution sensors. As cameras are updated video analytics and digital signal processing incorporated into cameras may become the norm.

III. Framework to Assess Object-level Coding

In trying to assess a Privacy Enhancing Technology (PET), it seems appropriate to turn to established Privacy Principles. These Privacy principles provide at least one lens to inform whether a new technology 'enhances' privacy. Particularly appropriate to any PET are the following four privacy principles first entrenched in the US Privacy Act (1974):

1. Accuracy:
Does the system help reduce errors or improve accuracy?
Does the system introduce new sources of potential error?

2. Access:
Does the system provide appropriate access?
Does the system allow for access control / managment?

3. Security:
Is the system as secure as, or more secure, than existing solutions?

4. Accountability:
Does the system provide mechanisms for improved oversight and compliance?

These principles serve as the framework for assessing face de-identification through Object-Level-Encoding as a Privacy Enhancing Technology.

IV. Evaluation of Object Level Encoding (Xiris Solution)

Background

Secure Object Level Coding is a technique developed at the University of Toronto that is currently undergoing commercialization (Martin and Plataniotis, 2008) by Engineered Privacy Inc. (EPI). EPI is a joint venture between Xiris Automation Inc. and the University of Toronto and Martin and Plataniotis continue as contributors. Their system employs secure visual object coding to encrypt objects identified in an image on a separate information layer. The encrypted object is then obscured on the original image layer. Combined with face detection this approach allows the privacy of individuals to be protected while retaining all data for retrieval with the proper access controls.

This software allows objects detected in video signals, like bodies and faces, to be obscured. What an “operator” sees is simply a blob (or any other graphic, logo, or image) instead of a face (see figure 1). This software may be performed on a chip built into a surveillance camera or performed before storage or viewing (not unlike the Bosch camera discussed above). Performing the encryption before transmission or storage would provide for optimal privacy protection. For example, Figure 1 is part of footage provided as part of a PIR. The video includes images of other people who have not been de-identified. Figure 2: shows an image of a woman with a stroller whose data was provided as part of the PIR. The footage provided has no faces obscured and hence a privacy violation. Using the system by EPI even faces at the back of the frame are obscured.

Figure 1: Obscured faces

Figure 2: Face in the Crowd

Object-level Encoding detects faces in video and replaces them with other information. In Figure 1, the system has detected the faces of several of the subway passengers and has replaced them with a white mask. The face data within the white masks is secured through an encryption algorithm and then either added on a separate layer of video for transmission or stored separately from what the "operator" sees. In the case of police warrant for the data, a system administrator may be asked to provide the "key" to the system and the face data can be decoded and reintegrated to create the original data image. The entire process only adds approximately 5% overhead, or additional bandwidth to the original data stream from a surveillance camera (depending on the number of faces and their relative size and duration in the video).

Figure 3: Still image from original PIR video of the Principal Investigator

When processed using the systems being developed by EPI the same video masks out facial information. As the PI comes into the frame a white mask instantly blocks out his facial features. Anyone viewing the video without proper permission would not be able to see more than the image below (Figure 4). However, when proper passwords are entered the image can be restored to its original form.

Figure 4: White mask obscures face in processed video

Secure object level encoding allows for privacy by default and access to the visual data only using proper permissions or access control. However, its effectiveness depends in part on the function of the overall system. For example if the face detection modules have difficulty detecting faces at angles between a face profile and an direct (forward) orientation, then portions of the final 'encoded' data my not fully obscure faces in the video at these angles. This then may lead to only partial information encoding and there may be frames where faces are partially visible (see Figure 4).

Figure 5: Limits to Masking

Although this limitation is relatively minor compared to entirely unprotected images--especially since subject's face is already partially obscured by the jacket—this may raise the concern that super-sampling the image may one day allow possible de-identification without proper permission. However it is likely that this limitation will be improved as the system is further developed. Furthermore an easy way around this is to apply secure coding to the entire body rather than just a face. Entire bodies, moving objects or events may be obscured and replaced by background data from other frames. This approach could be used to obscure all visual data in a frame that is not part of the background.

In Situ Testing

The above stills from the PIR video were processed in a controlled setting on at the company labs. We invited the company to a research day. The images in Figure 6 and 7 are the unprocess and processed stills from video captured that day.

Figure 6: Research Day audience

Figure 7: Audience after Encryption

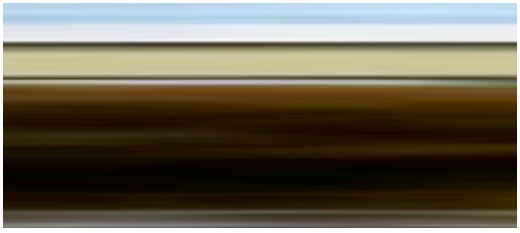


Figure 9: Background obscured

The above still demonstrate the potential of this system for encrypting privacy on a secure protected video information layer. The algorithm also demonstrates that it is not without some kinks. Figure 8 demonstrates a frame where the system mistakenly obscured an area above the individual's cup. However since the video information is still preserved on a separate layer and not changed in any

way, the accuracy of the original information is uncompromised. So although the system may itself have limitations currently (also see figure 5), and some infromation is not properly processed, it has no fundamental effect on the accuracy of the video information origially recorded when the process is reversed and the information is decrypted.

Access:
Since the system is designed to place personal infromation on a data layer separate from the original video layer it introduces a level of access control that the unprocessed video does not contain. The encryption and obscuring of the visual information prevents unautherized (re)viewing and can introduce a granular level of access control. The system can be set to obscure all but one specific face or a series of faces throughout a video sequence. If faces that are obscured are accessed without proper permissions, the image will only show as noise.

Security:
First it should be said that the video encoding portion of the overall security infrastructure is only as secure as other parts of the system. The strategy Xiris is proposing is most effective when incorporated at the video capture stage. If the de-identification is done on a chip built into the camera then the transmission of the video through IP and wireless networks becomes considerably more secure. If however the software is applied at the server or client side of the monitoring, then the storage and subsequent access may be considered more secure, but the transmission of the personal video information remains unaffected.

Accountability:
Accountability is arguably the principle most changed by the implementation of a deidentification system like Object-level Coding. With the ability to establish multiple information hierarchies and multiple levels of access to the encoded information if deployed as part of an infrastructure that promotes privacy and accountability the Xiris system imposes accountability on video surveillance systems—no individual can view the encoded data without proper permissions as well as recorded logs of the activity. However, with multiple layered accountibility and information coding it may become more difficult for individuals to gain access to their specific records as the information custodians intentionally or unintentionally make information requests harder to execute.

Overall, when deployed in a privacy sensitive framework face de-identification as a privacy enhancing strategy will likely prevent unauthorized access without compromising security. Once the viability of this technique is established, then by the data minimization principle those that do not incorporate this feature will be non-compliant, and potentially forced to adopt de-identification as the standard.

Works Cited

Bojkovic, Z. and A. Samcovic (2006).Face detection approach in neural network based method for video surveillance.

Cai, Y., D. Kaufer, et al. (2009). Semantic Visual Abstraction for Face Recognition Computational Science - Iccs 2009, Part I. G. Allen, J. Nabrzyski, E. Seidelet al. **5544:** 419-428.

Dixon, P., (2010). The *One-Way-Mirror Society:* Privacy Implications of the new Digital Signage Networks. World Privacy Forum. www.ftc.gov/os/comments/privacyroundtable/544506-00112.pdf *Retrieved: February 10, 2011.*

Gorodnichy, D. O. and E. Dubrofsky (2010). "VAP/VAT: Video Analytics Platform and Testbed for testing and deploying video analytics." Proceedings of SPIE-The International Society for Optical Engineering**7709**(Journal Article): 77090T-77090T.

Introna, L. D. and D. Wood (2004)."Picturing Algorithmic Surveillance: the politics of facial recognition systems."Surveillance & Society**2**(2/3): 177-198.

Introna, L. D. and H. Nissenbaum (2009).**Facial Recognition Technology:** A Survey of Policy and Implementation Issues, Lancaster University, UK; Centre for the Study of Technology and Organization.

Martin, K., Plataniotis, K., “Privacy Protected Surveillance Using Secure Visual Object Coding”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 18, pp. 1152-1162, 2008.

Norris, C. and M. McCahill (2006). "CCTV: Beyond penal modernism?" British Journal of Criminology**46**(1): 97-118.

Appendix A. Survey & Taxonomy of Video Analytics

Where is the state of the art?

Understating Video Analytics as a series of tasks allows for a selective review of research in areas including signal process, object recognition and classification, etc., to gain a sense of the state of the art in the field. Video analytic software may be divided into more developed activities (modules in the process chain) and higher level functions. The more established activities include signal processing of image quality, and automated object detection, tracking, recognition and classification.

Signal processing

Signal processing is itself a robust engineering area of research that includes a range of strategies to analyze and improve the quality of an image or video. Signal processing also referred to as Digital Signal Processing, is used to refer to a range of software and hardware systems that reduce signal noise, improve contrast and picture quality or improve data compression or transmission.

Ablavsky, V., M. Snorrason, et al. (2002).Real-time autonomous video enhancement system (RAVE).Image Processing. 2002. Proceedings. 2002 International Conference on.

The ability to autonomously enhance low-quality or corrupted streaming video data is essential in a number of important civilian and defense scenarios. Applications include visual surveillance, motion picture restoration, and remote control of unmanned aerial vehicles. We have developed a prototype of RAVE: real-time autonomous video enhancement system. It consists of a suite of video artifact detection algorithms and corresponding correction algorithms. The system is autonomously controlled by an intelligent software agent. Our prototype has been successfully validated on several video sequences from different application domains and is being matured into a fully-functional, real-time embedded system.

Deligiannidis, L., A. P. Sheth, et al. (2006). Semantic analytics visualization Intelligence and Security Informatics, Proceedings. 3975: 48-59.

Dockstader, S. L. and M. Tekalp (2001). "On the tracking of articulated and occluded video object motion." Real-Time Imaging 7(5): 415-432.

Kage, H., M. Seki, et al. (2007). Pattern recognition for video surveillance and physical security.

Kim, J. O., J. S. Kim, et al. (2005). "On a video surveillance system with a DSP by the LDA algorithm." LECTURE NOTES IN COMPUTER SCIENCE 3597(Journal Article): 200-207.

Lin, L., M. L. Shyu, et al. (2009). Mining High-Level Features from Video using Associations and Correlations.

Manap, N. A., G. Di Caterina, et al. (2010). Smart surveillance system based on stereo matching algorithms with IP and PTZ cameras. 3DTV-Conference: The True Vision - Capture, Transmission and Display of 3D Video (3DTV-CON), 2010.

In this paper, we describe a system for smart surveillance using stereo images with applications to advanced video surveillance systems. The system utilizes two smart IP cameras to obtain the position and location of objects. In this case, the object target is human face. The position and location of the object are automatically extracted from two IP cameras and subsequently transmitted to an ACTi Pan-Tilt-Zoom (PTZ) camera, which then points and zooms to the exact position in space. This work involves video analytics for estimating the location of the object in a 3D environment and transmitting its positional coordinates to the PTZ camera. The research consists of algorithms development in surveillance system including face detection, block matching, location estimation and implementation with ACTi SDK tool. The final system allows the PTZ camera to track the objects and acquires images in high-resolution quality.

Object Tracking

Another significant area of research particular to video analytics is object tracking between frames. Even when a system detects an 'object' in a frame, in real-time video signals, systems face the challenge of then tracking a particular object or multiple objects between video frames.

Amer, A. (2005). "Voting-based simultaneous tracking of multiple video objects." Circuits and Systems for Video Technology, IEEE Transactions on 15(11): 1448-1462.

This paper proposes an automatic object tracking method based on both object segmentation and motion estimation for real-time content-oriented video applications. The method focuses on the issues of speed of execution and reliability in the presence of noise, coding artifacts, shadows, occlusion, and object split. Objects are tracked based on the similarity of their features in successive frames. This is done in three steps: feature extraction, object matching, and feature monitoring. In the first step, objects are segmented and their spatial and temporal features are computed. In the second step, using a nonlinear two-stage voting strategy, each object of the previous frame is matched with an object of the current frame creating a unique correspondence. In the third step, object changes, such objects occlusion or split, are monitored and object features are corrected. These new features are then used to update results of previous steps creating module interaction. The contributions in this paper are the real-time two-stage voting strategy, the monitoring of object changes to handle occlusion and object split, and the spatiotemporal adaptation of the tracking parameters. Experiments on indoor and outdoor video shots containing over 6000 frames, including deformable objects, multi-object occlusion, noise, and coding and object segmentation artifacts have demonstrated the reliability and real-time response of the proposed method.

Chun-Ming, L., L. Yu-Shan, et al. (2005). Moving object segmentation and tracking in video. Machine Learning and Cybernetics, 2005.Proceedings of

2005 International Conference on.

Cossalter, M., M. Tagliasacchi, et al. (2009). Privacy-Enabled Object Tracking in Video Sequences Using Compressive Sensing. Advanced Video and Signal Based Surveillance, 2009. AVSS '09.Sixth IEEE International Conference on.

In this paper we propose a new coding scheme suitable for video surveillance applications that allows tracking of video objects without the need to reconstruct the sequence,thus enabling privacy protection. By taking advantage of recent findings in the compressive sensing literature, we encode a video sequence with a limited number of pseudo-random projections of each frame. At the decoder, we exploit the sparsity that characterizes background subtracted images in order to recover the location of the foreground object. We also leverage the prior knowledge about the estimated location of the object, which is predicted by means of a particle filter, to improve the recovery of the foreground object location. The proposed framework enables privacy, in the sense it is impossible to reconstruct the original video content from the encoded random projections alone, as well as secrecy, since decoding is prevented if the seed used to generate the random projections is not available.

Guo, L. and Y. Zhang (2006).Video Object Tracking Method Based on Snake Model Using Object's Histogram Information.Communications, Circuits and Systems Proceedings, 2006 International Conference on.

Jian, W., Y. Heng-jun, et al. (2010). Video Object Tracking Method Based on Normalized Cross-correlation Matching. Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium on.

Combing with specific temporal information of video, this paper proposes a kind of video object tracking method based on normalized cross-correlation matching by using the high precision characteristics of normalized cross-correlation image matching. Firstly, extract video background from the temporal information of video. Then, acquire the region of moving object using background subtraction. Lastly, carry out related matching and updating towards the extracted moving object by means of normalized cross-correlation. Experimental result shows that the adaptability of our method is strong, which can well solve the tracking problems when tracking objects have scale transform. It also has good anti-interference ability and robustness, and can track moving objects accurately under the condition of noise interference, lens dithering and background mutation.

Khan, Z. H., I. Y. H. Gu, et al. (2009). Joint anisotropic mean shift and consensus point feature correspondences for object tracking in video. Multimedia and Expo, 2009.ICME 2009.IEEE International Conference on.

We propose a novel tracking scheme that jointly employs point feature correspondences and object appearance similarity. For selecting point correspondences, we use a subset of scale-invariant point features from

SIFT that agree with a pre-defined affine transformation. The selected consensus points are then used for pre-selecting candidate regions. For appearance similarity based tracking, we employ an existing anisotropic mean shift, from which the formula for estimating bounding box parameters (width, height, orientation and center) are derived. A switching criterion is utilized to handle the situation where only a small number of point correspondences is found. Experiments and evaluation are performed on tracking moving objects on videos where objects may contain partial occlusions, intersection, deformation and pose changes among other transforms. Our comparisons with two existing methods have shown that the proposed scheme has yielded marked improvement, especially in terms of reducing tracking drifts, of robustness to occlusions, and of tightness and accuracy of tracked bounding box.

Kim, T., S. Lee, et al. (2011). "Combined shape and feature-based video analysis and its application to non-rigid object tracking." Image Processing, IET 5(1): 87-100.

Many video object tracking systems use block matching algorithm (BMA) because of its simple computational structure and robust performance. The BMA, however, exhibits fundamental limitations resulting from non-rigid shapes and similar patterns to the background. The authors propose a combined shape and feature-based non-rigid object tracking algorithm, which is tightly coupled with an adaptive background generation to overcome the limit of block matching. The proposed algorithm is robust to the object's sudden movement or the change of features. This becomes possible by tracking both feature points and their neighbouring regions. Combination of background and shape boundary information significantly improves the tracking performance because the target object and the corresponding feature points on the boundary can be easily found. The shape control points (SCPs) are regularly distributed on the contour of the object, and the authors compare and update the centroid during the tracking process, where straying SCPs are removed, and the tracking continues with only qualified SCPs. As a result, the proposed method becomes free from potential failing factors such as spatio-temporal similarity between object and background, object deformation and occlusion, to name a few. Experiments have been performed using several in-house video sequences including various objects such as a moving robot, swimming fish and walking people. In order to demonstrate the performance of the proposed tracking algorithm, a number of experiments have been performed under noisy and low-contrast environment. For more objective comparison, performance evaluation of tracking surveillance 2002 data sets were also used.

Ritch, M. and N. Canagarajah (2007).Motion-Based Video Object Tracking in the Compressed Domain.Image Processing, 2007.ICIP 2007.IEEE International Conference on.

In this paper an algorithm for real-time unsupervised segmentation and tracking of a moving object is proposed. This is performed within the

compressed domain using motion information only. Initial object segmentation is done using iterative rejection, taking advantage of its computational efficiency. The system seeks to overcome its disadvantages, namely a delay in object macroblocks appearing after consistency checking and non-identification of macroblocks containing object boundaries, by taking a model based approach to object tracking. The output of iterative rejection is used to update the model after tracking has taken place in each frame. Experimental results on a number of MPEG-2 encoded sequences demonstrate its effectiveness in identifying and tracking an object of interest from a compressed video stream and that the system is better than purely using iterative rejection as a segmentation method.

Stamm, M. and K. J. R. Liu (2008). Live video object tracking and segmentation using graph cuts. Image Processing, 2008.ICIP 2008.15th IEEE International Conference on.
Graph cuts have proven to be powerful tools in image segmentation. Previous graph cut research has proposed methods for cutting across large graphs constructed from multiple layered video frames, resulting in an object being tracked across multiple frames. However, this research focuses on cutting graphs constructed from a prerecorded video sequence. In live video scenarios, frames cannot be layered to construct 3D volumes, since the contents of the subsequent frames are unknown. Instead, new graphs must be created and cut for each frame on demand. Resource limitations make this unfeasible on high-resolution videos. In addition, object tracking requires a method for incorporating the previous frame's object position and shape into the current graph. We propose a method for tracking and segmenting objects in live video that utilizes regional graph cuts and object pixel probability maps. The regionalization of the cuts around the tracked object will increase the speed of the tracker, and the object pixel probability maps will enable more flexible tracking.

Szczodrak, M., P. Dalka, et al. (2010).Performance evaluation of video object tracking algorithm in autonomous surveillance system.Information Technology (ICIT), 2010 2nd International Conference on.
Results of a performance evaluation of a video object tracking algorithm are presented. The method of moving object detection and tracking is based on background modelling with mixtures of Gaussian and Kalman filters. An emphasis is put on algorithm's efficiency with regards to its settings. Utilized methods of a performance evaluation based on a comparison of the algorithm output to manually prepared reference data are introduced. The experiments aimed at examining the performance achieved with various object detection algorithm parameter settings are presented and discussed.

Thirde, D. and G. Jones (2004). Hierarchical probabilistic models for video object segmentation and tracking. Pattern Recognition, 2004.ICPR 2004.Proceedings of the 17th International Conference on.

Wei, Y. and W. Badawy (2003). A novel zoom invariant video object tracking

algorithm (ZIVOTA). Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on.

Yi, L. and Y. F. Zheng (2005). "Video object segmentation and tracking using ψ-learning classification." Circuits and Systems for Video Technology, IEEE Transactions on 15(7): 885-899.

As a requisite of the emerging content-based multimedia technologies, video object (VO) extraction is of great importance. This paper presents a novel semiautomatic segmentation and tracking method for single VO extraction. Unlike traditional approaches, the proposed method formulates the separation of the VO from the background as a classification problem. Each frame is divided into small blocks of uniform size, which are called object blocks if the centering pixels belong to the object, or background blocks otherwise. After a manual segmentation of the first frame, the blocks of this frame are used as the training samples for the object-background classifier. A newly developed learning tool called ψ-learning is employed to train the classifier which outperforms the conventional Support Vector Machines in linearly nonseparable cases. To deal with large and complex objects, a multilayer approach constructing a so-called hyperplane tree is proposed. Each node of the tree represents a hyperplane, responsible for classifying only a subset of the training samples. Multiple hyperplanes are thus needed to classify the entire set. Through the combination of the multilayer scheme and ψ-learning, one can avoid the complexity of nonlinear mapping as well as achieve high classification accuracy. During the tracking phase, the pixel in the center of every block in a successive frame is classified by a sequence of hyperplanes from the root to a leaf node of the hyperplane tree, and the class of the block is identified accordingly. All the object blocks thus form the object of interest, whose boundary unfortunately is stair-like due to the block effect. In order to obtain the pixel-wise boundary in a cost efficient way, a pyramid boundary refining algorithm is designed, which iteratively selects a few informative pixels for class label checking, and reduces uncertainty about the actual boundary of the object. The proposed method has been applied on video sequences with various spatial and temporal characteristics, and experimental results demonstrate it to be effective, efficient, and robust.

Ying-Tung, H., C. Cheng-Long, et al. (2005). Robust Multiple Targets Tracking Using Object Segmentation and Trajectory Estimation in Video. Systems, Man and Cybernetics, 2005 IEEE International Conference on.

In this paper, a novel robust unsupervised video object tracking algorithm is proposed. The proposed algorithm combines several techniques: mathematical morphology, region growing, region merging, and trajectory estimation, for tracking several predetermined video objects, simultaneously. A modified mathematical morphological edge detector was employed to sketch the contour of the video frame; and an edge-based object segmentation algorithm was applied to the contour for partitioning the predetermined objects; moreover, according to the motion of the

objects, the proposed algorithm can estimate and partition the objects in following video frames, automatically. The proposed algorithm is also robustness against mobile cameras. The experimental results show that the proposed algorithm can precisely partition and track multiple video objects

Zhi, L., S. Liquan, et al. (2007).A Novel Video Object Tracking Approach Based on Kernel Density Estimation and Markov Random Field.Image Processing, 2007.ICIP 2007.IEEE International Conference on.
In this paper, we propose a novel video object tracking approach based on kernel density estimation and Markov random field (MRF). The interested video objects are first segmented by the user, and a nonparametric model based on kernel density estimation is initialized for each video object and the remaining background, respectively. A temporal saliency map is also initialized for each object to memorize the temporal trajectory. Based on the probabilities evaluated on the non-parametric models, each pixel in the current frame is first classified into the corresponding video object or background using the maximum likelihood criterion. Starting from the initial classification result, a MRF model that combines spatial smoothness and temporal coherency is selectively exploited to generate more reliable video objects. The nonparametric model and the temporal saliency map for each video object are updated and propagated for the future tracking. Experimental results on several MPEG-4 test sequences demonstrate the good segmentation performance of our approach.

Object recognition

Tracking an object between frames is compounded by the challenge of trying to 'recognize' dimensionally shifting shapes. Object recognition within images is a key part of real-time event detection and response. Research in this area is moving to object recognition on mobile devices to help with augmented reality applications.

Amer, A., E. Dubois, et al. (2002). Context-independent real-time event recognition: application to key-image extraction. Pattern Recognition, 2002.Proceedings.16th International Conference on.

Fuerstenberg, K. and V. Willhoeft (2001). Object tracking and classification using laserscanners-pedestrian recognition in urban environment. Intelligent Transportation Systems, 2001.Proceedings.2001 IEEE.
Current car safety systems are passive systems. Modern car assistance systems are based only on vehicle data. Future safety systems will also include object recognition in the near frontal area of the vehicle to detect dangerous situations. Therefore, special sensors and algorithms are needed. The paper discusses a system using a laserscanner and a video camera

Gal, L., M. Rudzsky, et al. (2010). "Video Event Modeling and Recognition in Generalized Stochastic Petri Nets." Circuits and Systems for Video Technology, IEEE Transactions on 20(1): 102-118.
In this paper, we propose the surveillance event recognition framework using Petri Nets (SERF-PN) for recognition of event occurrences in video.

The Petri Net (PN) formalism allows a robust way to express semantic knowledge about the event domain as well as efficient algorithms for recognizing events as they occur in a particular video sequence. The major novelties of this paper are extensions to both the modeling and the recognition capacities of the Object PN paradigm. The first contribution of this paper is the extension of the PN representational capacities by introducing stochastic timed transitions to allow modeling of events which have some variance in duration. These stochastic timed transitions sample the duration of the condition from a parametrized distribution. The parameters of this distribution can be specified manually or learned from available video data. A second representational novelty is the use of a single PN to represent the entire event domain, as opposed to previous approaches which have utilized several networks, one for each event of interest. A third contribution of this paper is the capacity to probabilistically predict future events by constructing a discrete time Markov chain model of transitions between states. The experiments section of the paper thoroughly evaluates the application of the SERF-PN framework in the event domains of surveillance and traffic monitoring and provides comparison to other approaches using the CAVIAR dataset , a standard dataset for video analysis applications.

Hoogs, A., J. Rittscher, et al. (2003). Video content annotation using visual analysis and a large semantic knowledgebase.Computer Vision and Pattern Recognition, 2003.Proceedings.2003 IEEE Computer Society Conference on.

We present a novel approach to automatically annotating broadcast video. To manage the enormous variety of objects, events and scenes in video problem domains such as news video, we couple generic image analysis with a semantic database, WordNet, containing huge amounts of real-world information. Object and event recognition are performed by searching WordNet for concepts jointly supported by image evidence and topic context derived from the video transcript. No object- specific or event-specific training is required, and only a few object models and detection algorithms are required to label much of the significant content of news video. The hierarchical structure of WordNet yields hierarchical recognition, dynamically tailored to the level of supporting image evidence. The potential of the approach is demonstrated by analyzing a wide variety of scenes in news video.

Nguyen Dang, B. (2009).Autonomous Learning for Tracking and Recognition.Computing and Communication Technologies, 2009.RIVF '09.International Conference on.

We present an efficient approach for autonomous learning an object model from video or image sequences. The idea is to employ online boosting technique to adaptively learn an object representation from only as few as one labeled training sample. Our main contributions are: (1) A robust updating strategy of a discriminative classifier, which allows effective learning of an object model for tracking and recognition; (2) Learning and

tracking are performed in a single procedure with possibility of reducing drifting and ability to recover tracking failure; and (3) a simple yet reliable framework for object recognition. Our main concern is to use the approach for the problem of hand and face tracking and gesture recognition. However, the proposed framework can be applied to other objects. Experiments on different data sets (publicity available) show the efficiency of our approach over very recent published approaches on different objects.

Shuji, Z., F. Precioso, et al. (2010). STTK-based video object recognition. Image Processing (ICIP), 2010 17th IEEE International Conference on.
In this paper, we extend our video object recognition system to multiclass object recognition context, dealing with unbalanced data sets and comparing our resuls to state-of-the-art methods. Our approach is based on a Spatio-Temporal data representation, a dedicated kernel design and statistical learning techniques for object recognition. From video tracks made of segmented object regions in the successive frames, we extract sets of spatio-temporally coherent SIFT-based features, called Spatio-Temporal Tubes. To compare these complex tube objects, we integrate a Spatio-Temporal Tube Kernel (STTK) function into a multi-class classification framework with balancing process for unequal classes. Our approach is successfully evaluated on episodes from “Buffy, the Vampire Slayer” TV series which have been used in other works targeting same objectives. Our method proved to be more robust than dictionary based, facial feature based and key-frame based approaches. Our method is also tested on a small car database and preliminary results for car identification task illustrate its generalization potential.

Taehee, L. and S. Soatto (2010). Feature tracking and object recognition on a hand-held. Mixed and Augmented Reality (ISMAR), 2010 9th IEEE International Symposium on.
We demonstrate a visual recognition system operating on a hand-held device, with the help of an efficient and robust feature tracking and an object recognition mechanism that can be used for interactive mobile applications. In our recognition system, corner features are detected from captured video frames in a multi-scale image pyramid, and are tracked between consecutive frames efficiently. In order to perform object recognition, local descriptors are calculated on the tracked features, and quantized using a vocabulary tree. For each object, a bag-of-words model is learned from multiple views. The learned objects are recognized by computing the ranking score for the set of features in a single video frame. Our feature tracking algorithm and local descriptors are different than the Lucas-Kanade algorithm in image pyramid or the SIFT descriptor, however improving the efficiency and accuracy. For our implementation on a mobile phone, we used an iPhone 3GS with a 600MHz ARM chip CPU. The video frame is captured from a camera preview screen at a rate of 15 frames per second using the public API. The task of object recognition on a mobile phone runs at around 7 frames per second, including the feature tracking

and descriptor calculation.
Tan, F., Q. Guan, et al. (2009).A method for robust recognition and tracking of multiple objects.Communications, Circuits and Systems, 2009.ICCCAS 2009.International Conference on.
This paper presents an accurate and flexible method for robust recognition and tracking of multiple objects in video sequence. We calculate color moments and wavelet moments for each detected object. Based on the extracted moment features, the SVM achieves optimal object recognition performance. The object recognition rate is above 98.53%. Since the tracking accuracy of feature matching method could be degraded by occlusion, we add a Kalman filter tracking framework based on object recognition to improve multiple objects tracking. The previous object recognition module improves the performance and the accuracy of the Kalman filter tracking framework. Results obtained suggest that our tracking algorithm is very effective and robust even in challenging tracking conditions like occlusion and background clutter.
Tie, L., Y. Zejian, et al. (2011)."Learning to Detect a Salient Object." Pattern Analysis and Machine Intelligence, IEEE Transactions on 33(2): 353-367.
In this paper, we study the salient object detection problem for images. We formulate this problem as a binary labeling task where we separate the salient object from the background. We propose a set of novel features, including multiscale contrast, center-surround histogram, and color spatial distribution, to describe a salient object locally, regionally, and globally. A conditional random field is learned to effectively combine these features for salient object detection. Further, we extend the proposed approach to detect a salient object from sequential images by introducing the dynamic salient features. We collected a large image database containing tens of thousands of carefully labeled images by multiple users and a video segment database, and conducted a set of experiments over them to demonstrate the effectiveness of the proposed approach.
Walls, B. (2010)."Cascaded Automatic Target Recognition (Cascaded ATR)." Proceedings of SPIE-The International Society for Optical Engineering 7696(Journal Article): 76960W-76960W.
Wechsler, H. (2007). Robust Recognition-by-Parts Using Transduction and Boosting with Applications to Biometrics. Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop on.

Event recognition

Another area of research included in Video Analytics is event recognition. Even recognition allows for the automatic (usually contextual) interpretation of recognizable objects over time. This area of research spans a range of application domains from fire-alarms to theft prevention.

"Smart CCTV raises bush-fire alarm." New Scientist 205(2749): 19-19.
Abrams, D., S. McDowall, et al. (2007).Video content analysis with effective

response.
Loney, G. (2007). Border Intrusion Detection: Thinking outside the perimeter. Security Technology, 2007 41st Annual IEEE International Carnahan Conference on.
Maciejewski, R., S. Kim, et al. (2008). Situational awareness and visual analytics for emergency response and training.
Pratl, G., L. Frangu, et al. (2007). Smart nodes for semantic analysis of visual and aural data. 2007 5th Ieee International Conference on Industrial Informatics, Vols 1-3: 1027-1032.
Venkoparao, V. G., R. N. Hota, et al. (2009). Flare Monitoring for Petroleum Refineries.
Wang, Y. and G. Mori (2010). "Hidden Part Models for Human Action Recognition: Probabilistic vs. Max-Margin." Pattern Analysis and Machine Intelligence, IEEE Transactions on PP(99): 1-1.
We present a discriminative part-based approach for human action recognition from video sequences using motion features. Our model is based on the recently proposed hidden conditional random field~(HCRF) for object recognition. Similar to HCRF for object recognition, we model a human action by a flexible constellation of parts conditioned on image observations. Different from object recognition, our model combines both large-scale global features and local patch features to distinguish various actions. Our experimental results show that our model is comparable to other state-of-the-art approaches in action recognition. In particular, our experimental results demonstrate that combining large-scale global features and local patch features performs significantly better than directly applying HCRF on local patches alone. We also propose an alternative for learning the parameters of an HCRF model in a max-margin framework. We call this method the max-margin hidden conditional random field~(MMHCRF). We demonstrate that MMHCRF outperforms HCRF in human action recognition. In addition, MMHCRF can handle a much broader range of complex hidden structures arising in various problems in computer vision.
Asif, M. and J. Soraghan (2008)."Video Analytics for Panning Camera in Dynamic Surveillance Environment." MONOGRAPH OF THE COTSEN INSTITUTE OF ARCHAELOGY, UCLA(Journal Article): 79-82.
Janoos, F., S. Singh, et al. (2007). Activity Analysis Using Spatio-Temporal Trajectory Volumes in Surveillance Applications.Visual Analytics Science and Technology, 2007.VAST 2007.IEEE Symposium on.
In this paper, we present a system to analyze activities and detect anomalies in a surveillance application, which exploits the intuition and experience of security and surveillance experts through an easy- to-use visual feedback loop. The multi-scale and location specific nature of behavior patterns in space and time is captured using a wavelet-based feature descriptor. The system learns the fundamental descriptions of the behavior patterns in a semi-supervised fashion by the higher order singular value decomposition of the space described by the training data.

This training process is guided and refined by the users in an intuitive fashion. Anomalies are detected by projecting the test data into this multi-linear space and are visualized by the system to direct the attention of the user to potential problem spots. We tested our system on real-world surveillance data, and it satisfied the security concerns of the environment.

Marraud, D., B. Cepas, et al. (2009). Semantic Browsing of Video Surveillance Databases through Online Generic Indexing.

Venkoparao, V. G., R. N. Hota, et al. (2009). Flare Monitoring for Petroleum Refineries.

Human tracking

Object tracking and recognition are only a few of the modules that contribute to Human tracking, a basic requirement for analysing human behaviours in retail settings for example. When the object tracking and classification modules code an object or objects in the foreground as human or parts of a human, then other modules take over to perform such tasks as tracking the individual across frames, between cameras and record and analyze information like gender, age and even ethnicity in addition to other biometrics such as gait and physiological or behavioural based identification.

Bocchetti, G., F. Flammini, et al. (2009). Dependable integrated surveillance systems for the physical security of metro railways.

Dawson, D., P. Derby, et al. (2009). A Report on Camera Surveillance in Canada: Part Two. Kingston, Queen's University

De Angelis, D., R. Sala, et al. (2009). "A new computer-assisted technique to aid personal identification." International journal of legal medicine 123(4): 351-356.

Deisman, W., P. Derby, et al. (2009). A Report on Camera Surveillance in Canada: Part One. Kingston, Queen's University.

Dixon, P. (2010). The One-Way-Mirror Society: Privacy Implications of the new Digital Signage Networks, World Privacy Forum.

Elder, J. H., S. J. D. Prince, et al. (2007)."Pre-attentive and attentive detection of humans in wide-field scenes." International Journal of Computer Vision 72(1): 47-66.

Everingham, M. and A. Zisserman (2005).Identifying individuals in video by combining 'generative' and discriminative head models.Computer Vision, 2005.ICCV 2005.Tenth IEEE International Conference on.

The objective of this work is automatic detection and identification of individuals in unconstrained consumer video, given a minimal number of labelled faces as training data. Whilst much work has been done on (mainly frontal) face detection and recognition, current methods are not sufficiently robust to deal with the wide variations in pose and appearance found in such video. These include variations in scale, illumination, expression, partial occlusion, motion blur, etc. We describe two areas of innovation: the first is to capture the 3-D appearance of the entire head, rather than just the face region, so that visual features such as the hairline

can be exploited. The second is to combine discriminative and 'generative' approaches for detection and recognition. Images rendered using the head model are used to train a discriminative tree-structured classifier giving efficient detection and pose estimates over a very wide pose range with three degrees of freedom. Subsequent verification of the identity is obtained using the head model in a 'generative' framework. We demonstrate excellent performance in detecting and identifying three characters and their poses in a TV situation comedy

Gagnon, L., F. Laliberte, et al. (2006). "A system for tracking and recognizing pedestrian faces using a network of loosely coupled cameras - art. no. 62460N." PROCEEDINGS OF THE SOCIETY OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS (SPIE) 6246(Journal Article): N2460-N2460.

Greenberg, J. and S. P. Hier (2009)."CCTV Surveillance and the Poverty of Media Discourse." Canadian Journal of Communication 34(3): 461-486.

Saptharishi, M. and D. Marman (2009). An Information Value Driven Architecture for Urban Video Surveillance in Data and Attention Bandwidth Constrained Environments.

Candamo, J., M. Shreve, et al. (2010). "Understanding Transit Scenes: A Survey on Human Behavior-Recognition Algorithms." Ieee Transactions on Intelligent Transportation Systems 11(1): 206-224.

Chen, Y., Z. Yiwen, et al. (2008). Visual mining of multimedia data for social and behavioral studies.Visual Analytics Science and Technology, 2008.VAST '08.IEEE Symposium on.

With advances in computing techniques, a large amount of high-resolution high-quality multimedia data (video and audio, etc.) has been collected in research laboratories in various scientific disciplines, particularly in social and behavioral studies. How to automatically and effectively discover new knowledge from rich multimedia data poses a compelling challenge since state-of-the-art data mining techniques can most often only search and extract pre-defined patterns or knowledge from complex heterogeneous data. In light of this, our approach is to take advantages of both the power of human perception system and the power of computational algorithms. More specifically, we propose an approach that allows scientists to use data mining as a first pass, and then forms a closed loop of visual analysis of current results followed by more data mining work inspired by visualization, the results of which can be in turn visualized and lead to the next round of visual exploration and analysis. In this way, new insights and hypotheses gleaned from the raw data and the current level of analysis can contribute to further analysis. As a first step toward this goal, we implement a visualization system with three critical components: (1) A smooth interface between visualization and data mining. The new analysis results can be automatically loaded into our visualization tool. (2) A flexible tool to explore and query temporal data derived from raw multimedia data. We represent temporal data into two forms - continuous variables and event variables. We have developed various ways to visualize both

temporal correlations and statistics of multiple variables with the same type, and conditional and high-order statistics between continuous and event variables. (3) A seamless interface between raw multimedia data and derived data. Our visualization tool allows users to explore, compare, and analyze multi-stream derived variables and simultaneously switch to access raw multimedia data. We de- - monstrate various functions in our visualization program using a set of multimedia data including video, audio and motion tracking data.

Hampapur, A., R. Bobbitt, et al. (2009). Video Analytics in Urban Environments.

Jones, C., M. Ogawa, et al. (2009). VIDI surveillance - embassy monitoring and oversight system.Visual Analytics Science and Technology, 2009.VAST 2009.IEEE Symposium on.

Human Identification

Though not necessary for all application domains involving human tracking and behaviour analysis, video analytics also includes strategies for human identification using video data. A particular focus of human identification has been HumanID at a distance. The face features prominently among other identification or biometric strategies like gait recognition, with a large number of contributing research strands. Face Recognition a significant focus of computer vision over the last decade is itself a composite of modular research areas the stretch back into the 1970's. Face Recognition Technologies (FRT) include face detection, tracking and recognition solutions.

Face detection

Solutions for detecting faces in visual date may be trased back to the 1970's (Gates, 2004) and existing algorithms found on commercial cameras and phones are robust and feature rich. However research continues in this area to improve the scope and accuracy of identifying faces from various angles, under differing conditions and of multiple subjects.

Alajel, K. M., W. Xiang, et al. (2010). "Face Detection Technique Based on Skin Color and Facial Features." Mathematics and Computers in Science and Engineering(Journal Article): 192-199.

Bao, P. T., J. Y. Kim, et al. (2005). "Fast multi-face detection in color images using fuzzy logic." International Symposium on Intelligent Signal Processing and Communication Systems-ISPACS(Journal Article): 777-780.

Bojkovic, Z. and A. Samcovic (2006). Face detection approach in neural network based method for video surveillance.

Chen, T.-W., W.-K.Chan, et al. (2007).Efficient face detection with segmentation and feature-based face scoring in surveillance systems.

Dockstader, S. L. and A. M. Tekalp (2000). "Real-time object tracking and human face detection in cluttered scenes." PROCEEDINGS OF THE SOCIETY OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS (SPIE) 3974(Journal Article): 957-968.

Elder, J. H., S. J. D. Prince, et al. (2007)."Pre-attentive and attentive detection of

humans in wide-field scenes." International Journal of Computer Vision 72(1): 47-66.
Feris, R. S., T. E. de Campos, et al. (2000). "Detection and tracking of facial features in video sequences." LECTURE NOTES IN ARTIFICIAL INTELLIGENCE 1793(Journal Article): 127-135.
Hjelmas, E. and B. K. Low (2001). "Face detection: A survey." Computer Vision and Image Understanding 83(3): 236-274.
Hota, R. N., V. Venkoparao, et al. (2006). Face detection by using skin color model based on one class classifier.
Hsu, R. L., M. Abdel-Mottaleb, et al. (2002). "Face detection in color images." IEEE Transactions on Pattern Analysis and Machine Intelligence 24(5): 696-706.
Karungaru, S., M. Fukumi, et al. (2009)."DETECTION AND RECOGNITION OF VEHICLE LICENSE PLATES USING TEMPLATE MATCHING, GENETIC ALGORITHMS AND NEURAL NETWORKS." International Journal of Innovative Computing Information and Control 5(7): 1975-1985.
Kim, J. B., Y. H. Sung, et al. (2004). A fast and robust face detection based on module switching network.
Kim, J. O. and J. S. Kim (2005)."Real-time implementation of face detection for a ubiquitous computing." LECTURE NOTES IN COMPUTER SCIENCE 3480(Journal Article): 1187-1195.
Kim, J. O., S. J. Seo, et al. (2004). "Face detection by facial features with color images and face recognition using PCA." LECTURE NOTES IN COMPUTER SCIENCE 3043(Journal Article): 1-8.
Kim, T. K., S. U. Lee, et al. (2002). "Integrated approach of multiple face detection for video surveillance." INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION(Journal Article): 394-397.
Lin, D.-T.and M.-J. Liu (2006). "Face occlusion detection for automated teller machine surveillance." LECTURE NOTES IN COMPUTER SCIENCE 4319(Journal Article): 641-651.
Liu, Z. F., Z. S. You, et al. (2003). Face detection and facial feature extraction in color image.
Loney, G. (2007). Border Intrusion Detection: Thinking outside the perimeter. Security Technology, 2007 41st Annual IEEE International Carnahan Conference on.
Detecting infiltration across national borders is not simply a matter of deploying commercial-off-the-shelf perimeter intrusion sensors. The sheer length of border systems has led some to propose using wide area surveillance systems to reduce cost. Unfortunately the most common of these technologies: thermal infrared and visible wavelength sensors integrated with video analytics and ground radar have line-of-sight limitations and less than optimum nuisance alarm characteristics for real world border applications. The missing link is a cost-effective terrain following trip-wire sensor to cue these wide-area systems and mitigate their performance limitations. Buried ported coax, sometimes called leaky coax or guided radar sensors have protected high value perimeters for

over two decades. In theory, their high probability of detection, resistance to defeat and vandalism, invisible terrain following volumetric field and good nuisance alarm characteristics make them well suited to secure borders; but their high cost per zone and inability to accommodate different soil conditions have argued against their use. OmniTrax¿ is a new ultra wideband spread spectrum ranging guided radar which changes this equation with a lower cost per zone, one-meter target resolution and the ability to accommodate different soil types. Ongoing research may eventually result in the ability to track targets along the cables, determine the direction of travel of targets crossing the cables, surface mount the sensor cables in rocky terrain and cost effectively install the sensor cables in soil or sand using cable plows; any of which would only improve the technology's utility in border intrusion detection.

Lu, Y. Z., J. L. Zhou, et al. (2003). "A survey of face detection, extraction and recognition." Computing and Informatics 22(2): 163-195.

Manap, N. A., G. Di Caterina, et al. (2010). Face detection and stereo matching algorithms for smart surveillance system with IP cameras. Visual Information Processing (EUVIP), 2010 2nd European Workshop on.
In this paper, we describe a smart surveillance system to detect human faces in stereo images with applications to advanced video surveillance systems. The system utilizes two smart IP cameras to obtain the position and location of the object that is a human face. The position and location of the object are extracted from two IP cameras and subsequently transmitted to a Pan-Tilt-Zoom (PTZ) camera, which can point to the exact position in space. This work involves video analytics for estimating the location of the object in a 3D environment and transmitting its positional coordinates to the PTZ camera. The research consists of algorithm development in surveillance system including face detection, stereo matching, location estimation and implementation with ACTi PTZ camera. The final system allows the PTZ camera to track the objects and acquires images in high-resolution.

Miao, L. G., F. W. Wang, et al. (2009). Automatic License Plate Detection Based on Edge density and Color Model.

Nallaperumal, K., R. Subban, et al. (2006). Human face detection in color images using skin color and template matching models for multimedia on the web.

Oancea, R., S. Kifor, et al. (2009). Considerations on Skin Colour Algorithms used for Candidate Faces Detection.

Pai, Y.-T., S.-J.Ruan, et al. (2006).A simple and accurate color face detection algorithm in complex background.

Park, S. H., E. Y. Kim, et al. (2001). Face detection for security system on the Internet.

Phimoltares, S., C. Lursinsap, et al. (2007). "Face detection and facial feature localization without considering the appearance of image context." Image and Vision Computing 25(5): 741-753.

Ravi Kumar, C. N. and A. Bindu (2006)."An efficient skin illumination compensation model for efficient face detection." IEEE Industrial

Electronics Society(Journal Article): 3298-3303.
Tie, Y. and L. Guan (2009). "Automatic face detection in video sequences using local normalization and optimal adaptive correlation techniques." Pattern Recognition 42(9): 1859-1868.
Zhang, Q., S.-i.Kamata, et al. (2009). Face Detection and Tracking in Color images Using Color Centroids Segmentation.
Zhang, Q. and Z.-J.Liu (2006). Face Detection based on complexional segmentation and feature extraction.
Zhang, Q., J. Zhang, et al. (2008). "Face detection method based on color barycenter hexagon model." Lecture Notes in Engineering and Computer Science(Journal Article): 655-658.
Zhao, L., X. Sun, et al. (2006). "Face detection based on facial features." International Conference on Signal Processing-ICSP(Journal Article): 1758-1761.
Zuo, F. and P. H. N. de With (2003). "Fast human face detection using successive face detectors with incremental detection capability." PROCEEDINGS OF THE SOCIETY OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS (SPIE) 5022(Journal Article): 831-841.

Face recognition

Detecting a face in an image or video clip is one challenge, but the ability to correctly associate face data with specific individuals is more challenge. Face Recognition is perhaps one of the most active frontiers of biometric research since 9/11.

Cai, Y., D. Kaufer, et al. (2009). Semantic Visual Abstraction for Face Recognition. Computational Science - Iccs 2009, Part I. G. Allen, J. Nabrzyski, E. Seidelet al. 5544: 419-428.
Cheung, K.-W., J. Chen, et al. (2008). Pose-tolerant Non-frontal Face Recognition using EBGM.
Choi, J. Y., Y. M. Ro, et al. (2008). Feature Subspace Determination in Video-based Mismatched Face Recognition.
Choi, J. Y., Y. M. Ro, et al. (2009). "Color Face Recognition for Degraded Face Images."Ieee Transactions on Systems Man and Cybernetics Part B-Cybernetics 39(5): 1217-1230.
Harguess, J., H. Changbo, et al. (2009). Fusing face recognition from multiple cameras.Applications of Computer Vision (WACV), 2009 Workshop on. Face recognition from video has recently received much interest. However, several challenges for such a system exist, such as resolution, occlusion (from objects or self-occlusion), motion blur, and illumination. The aim of this paper is to overcome the problem of self-occlusion by observing a person from multiple cameras with uniquely different views of the person's face and fusing the recognition results in a meaningful way. Each camera may only capture a part of the face, such as the right or left half of the face. We propose a methodology to use cylinder head models (CHMs) to track the face of a subject in multiple cameras. The problem of face recognition from video is then transformed to a still face recognition

problem which has been well studied. The recognition results are fused based on the extracted pose of the face. For instance, the recognition result from a frontal face should be weighted higher than the recognition result from a face with a yaw of 30Â°. Eigenfaces is used for still face recognition along with the average-half-face to reduce the effect of transformation errors. Results of tracking are further aggregated to produce 100% accuracy using video taken from two cameras in our lab.

Huang, H. and H.He (2011)."Super-Resolution Method for Face Recognition Using Nonlinear Mappings on Coherent Features." IEEE Transactions on Neural Networks 22(1): 121-130.

Huang, P. and Y. Wang (2009).The Impact of Changing Resolutions on Face Recognition.

Huang, Z.-K., W.-Z.Zhang, et al. (2008). Using Gabor Filters Features for Multi-Pose Face Recognition in Color Images.

Hulbert, W., C. Podilchuk, et al. (2008)."Face Recognition using a Pictorial-Edit Distance." IEEE International Conference on Image Processing (ICIP)(Journal Article): 1908-1911.

Jillela, R. R. and A. Ross (2009)."Adaptive Frame Selection for Improved Face Recognition in Low-Resolution Videos." IEEE International Joint Conference on Neural Networks (IJCNN)(Journal Article): 2835-2841.

Klare, B. and M. Burge (2010)."Assessment of H.264 Video Compression on Automated Face Recognition Performance in Surveillance and Mobile Video Scenarios." Proceedings of SPIE-The International Society for Optical Engineering 7667(Journal Article): 76670X-76670X.

Privacy Sensitive VA research

Despite the range of research in the areas of video analytics, proportionally little research actually incorporates privacy into the design. Notable exceptions are found below.

Coudert, F. and J. Dumortier (2008). Intelligent video surveillance networks: data protection challenges.

Gross, R., E. Airoldi, et al. (2006). "Integrating utility into face de-identification." LECTURE NOTES IN COMPUTER SCIENCE 3856(Journal Article): 227-242.

Matusek, F. and R. Reda (2008). Efficient Secure Storage of Privacy Enhanced Video Surveillance Data in Intelligent Video Surveillance Systems.

Matusek, F., R. Reda, et al. (2008). Efficient Secure Storage of Privacy Enhanced Video Surveillance Data in Intelligent Video Surveillance Systems.

Newton, E. M., L. Sweeney, et al. (2005). "Preserving privacy by de-identifying face images." IEEE Transactions on Knowledge and Data Engineering 17(2): 232-243.

Senior, A. (2008). "Privacy Enablement in a Surveillance System." IEEE International Conference on Image Processing (ICIP)(Journal Article): 1680-1683.

Senior, A. and Ieee (2008). PRIVACY ENABLEMENT IN A SURVEILLANCE SYSTEM. 2008 15th Ieee International Conference on Image Processing,

Vols 1-5: 1680-1683.
Vagts, H. and A. Bauer (2010).Privacy-Aware Object Representation for Surveillance Systems. Advanced Video and Signal Based Surveillance (AVSS), 2010 Seventh IEEE International Conference on.
Real-time object tracking, feature assessment and classification based on video are an enabling technology for improving situation awareness of human operators as well as for automated recognition of critical situations. To bridge the gap between video signal-processing output and spatio-temporal analysis of object behavior at the semantic level, a generic and sensor-independent object representation is necessary. However, in the case of public and corporate video surveillance, centralized storage of aggregated data leads to privacy violations. This article explains how a centralized object representation, complying with the Fair Information Practice Principles (FIP) privacy constraints, can be implemented for a video surveillance system.

"Smart" Video Surveillance

Higher level semantic decision driven responses using software are still being developed for deployment. A sample of some literature can be found below.

"Smart CCTV raises bush-fire alarm." New Scientist 205(2749): 19-19.
Abrams, D., S. McDowall, et al. (2007).Video content analysis with effective response.
Deligiannidis, L., A. P. Sheth, et al. (2006). Semantic analytics visualization.Intelligence and Security Informatics, Proceedings. 3975: 48-59.
Maciejewski, R., S. Kim, et al. (2008). Situational awareness and visual analytics for emergency response and training.
Pratl, G., L. Frangu, et al. (2007). Smart nodes for semantic analysis of visual and aural data. 2007 5th Ieee International Conference on Industrial Informatics, Vols 1-3: 1027-1032.
Venkoparao, V. G., R. N. Hota, et al. (2009). Flare Monitoring for Petroleum Refineries.

Automated Traffic Monitoring

A particularly active area of research in the area of video analytics includes traffic and transportation monitoring and Automated License-Plate Recognition or (ALPR). This form of analysis can range from tracking general patterns to specific violations, but can also be purposed to track movements of specific vehicles and by extension individuals.

Chen, Z. X., C. Y. Liu, et al. (2009). "Automatic License-Plate Location and Recognition Based on Feature Salience." Ieee Transactions on Vehicular Technology 58(7): 3781-3785.
Chen, Z. X., C. Y. Liu, et al. (2007). "Automatic license plate location and recognition." Indian Journal of Engineering and Materials Sciences 14(5): 337-345.
Fan, X., G. L. Fan, et al. (2007).Joint segmentation and recognition of license

plate characters. 2007 Ieee International Conference on Image Processing, Vols 1-7: 2049-2052.
Gonzalez, J., F. X. Roca, et al. (2009). "Research Steps Towards Human Sequence Evaluation." COMPUTATIONAL METHODS IN APPLIED SCIENCES 13(Journal Article): 105-115.
Huang, F., Z. M. Li, et al. (2008).A novel algorithm of character segmentation in vehicle license plates.
Kang, D. J. (2009). "DYNAMIC PROGRAMMING-BASED METHOD FOR EXTRACTION OF LICENSE PLATE NUMBERS OF SPEEDING VEHICLES ON THE HIGHWAY." International Journal of Automotive Technology 10(2): 205-210.
Karungaru, S., M. Fukumi, et al. (2009)."DETECTION AND RECOGNITION OF VEHICLE LICENSE PLATES USING TEMPLATE MATCHING, GENETIC ALGORITHMS AND NEURAL NETWORKS." International Journal of Innovative Computing Information and Control 5(7): 1975-1985.
Khan, N. Y., A. S. Imran, et al. (2007). Distance and color invariant automatic license plate recognition system.
Kulkarni, P., A. Khatri, et al. (2009). Automatic Number Plate Recognition (ANPR) System for Indian conditions.
Leibe, B., K. Schindler, et al. (2008). "Coupled Object Detection and Tracking from Static Cameras and Moving Vehicles." Pattern Analysis and Machine Intelligence, IEEE Transactions on 30(10): 1683-1698.
We present a novel approach for multi-object tracking which considers object detection and spacetime trajectory estimation as a coupled optimization problem. Our approach is formulated in a minimum description length hypothesis selection framework, which allows our system to recover from mismatches and temporarily lost tracks. Building upon a state-of-the-art object detector, it performs multiview/multicategory object recognition to detect cars and pedestrians in the input images. The 2D object detections are checked for their consistency with (automatically estimated) scene geometry and are converted to 3D observations which are accumulated in a world coordinate frame. A subsequent trajectory estimation module analyzes the resulting 3D observations to find physically plausible spacetime trajectories. Tracking is achieved by performing model selection after every frame. At each time instant, our approach searches for the globally optimal set of spacetime trajectories which provides the best explanation for the current image and for all evidence collected so far while satisfying the constraints that no two objects may occupy the same physical space nor explain the same image pixels at any point in time. Successful trajectory hypotheses are then fed back to guide object detection in future frames. The optimization procedure is kept efficient through incremental computation and conservative hypothesis pruning. We evaluate our approach on several challenging video sequences and demonstrate its performance on both a surveillance-type scenario and a scenario where the input videos are taken from inside a moving vehicle passing through crowded city areas.

Zopez, J., J. Gonzalez, et al. (2007). A versatile low-cost car plate recognition system.
Miao, L. G., F. W. Wang, et al. (2009). Automatic License Plate Detection Based on Edge density and Color Model.
Molder, C., M. Boscoianu, et al. (2008). Improved automatic number plate recognition system.Proceedings of the 1st Wseas International Conference on Visualization, Imaging and Simulation. M. Iliescu, R. I. Munteanu, J. FraustoSoliset al: 49-54.
Thornton, J., J. Baran-Gale, et al. (2009). An Assessment of the Video Analytics Technology Gap for Transportation Facilities.
Zidouri, A., M. Deriche, et al. (2008). RECOGNITION OF ARABIC LICENSE PLATES USING NN.