'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.