"I'll Be Watching You"

Awareness, Consent, Compliance and Accountability in Video Surveillance

Brenda McPhail, Andrew Clement, Joseph Ferenbok, and Arndis Johnson
Faculty of Information
University of Toronto
Toronto, Canada
{Brenda.McPhail} {Andrew.Clement}{Joseph.Ferenbok} @utoronto.ca, Arndis.Johnson@mail.utoronto.ca

Abstract— **This paper reports on-going, citizen-focussed research that seeks to a) understand what people know, and want to know, about the video surveillance they encounter; b) highlight the widespread privacy non-compliance of private sector video surveillance operators; and c) develop the means for citizens to hold surveillant organizations to public account. It combines in situ interviews, participatory design workshops and smartphone app development for probing surveillance practices while empowering concerned individuals to act collaboratively in better regulating video surveillance.**

Keywords-sousveillance; crowdsourced veillance; privacy; (non)compliance

I. Introduction

Anecdotally, most people know that the video technology we use in everyday life is changing at an alarmingly fast pace. Individuals see that the televisions they watch and the cameras they buy are increasingly of higher quality, increasingly versatile, and increasingly integrated with computing technologies. However, the same people who use these technologies to watch or record do not often actively think about what this means in connection with the technologies used to watch and record them. Most are similarly unaware of the networked infrastructures that may connect and add new functionality to the video surveillance systems that are collecting their personal information on a daily basis.

Or so we hypothesize. However, there is relatively little academic research that assesses the current level of public knowledge about video surveillance technologies and practices in North America. Furthermore, previous work conducted by members of our research group has determined that private-sector compliance with video surveillance privacy regulation is poor [2]. We believe this makes it particularly important to explore what citizens know and what they need to know, and provide them with the information and tools they need to effectively engage with the organisations that collect and use their personal information via surveillance. Our ultimate research goal is to provide information and tools to help members of the public think about and understand video surveillance technologies and the ways they are changing. We also hope to help citizens to engage thoughtfully with organizations engaged in surveillance, and with government policy makers and the policies that regulate this surveillance. We seek to find ways to make surveillance infrastructure issues vivid and concrete, to make tangible artifacts that people can use to open up the technologies, organizational practices and built-in assumptions that are most often hidden from public view. The issues we highlight include privacy, individual control over personal information, and the potential for citizens to hold organisations to account for protecting both of these important values.

Our research addresses these goals using two distinct but linked approaches: qualitative research to examine the current state of awareness and understanding that Canadians have about video surveillance, and participatory design-inspired prototyping work to develop simple and effective tools to help citizens to document surveillance installations in their local environment. This paper reports on the results of both of these approaches. We begin by discussing the preliminary findings from our qualitative study of Canadian's attitudes to, and awareness of, video surveillance. We conducted on-the-street interviews with Canadians, in an attempt to understand what people living in a Canadian urban center understand about video surveillance systems and privacy regulation. We then turn to our second, participatory design-oriented approach, which attempts to respond to people's concerns and information needs regarding video surveillance by developing a tool for individuals called the SurveillanceWatch app. This app uses a crowdsourcing approach to allow people to map sites of surveillance and record their compliance with privacy regulations. The design and nature of this app is discussed in the second section of this paper. Finally, we will conclude by integrating the discussions of these two research approaches and highlighting the key contributions of this work.

II. What do Canadians know or want to know about video surveillance?

Video surveillance is becoming ubiquitous in both private and public spaces in our increasingly (in)security-conscious contemporary society. But, although we still see the familiar camera housings on walls or ceilings, on the inside, the capabilities of video surveillance technologies have grown and changed over the past decade. As we move from analog to digital video on networked systems, we see the potential for an increasingly intensive gaze to be trained on citizens in the name of security. The move to digital processing also opens up the possibility that the visual image data collected might soon be turned into actionable information, either in real time or retrospectively through analysis of recorded aggregate data. Armed with object recognition, face tracking, and face recognition, visual surveillance will soon have the potential to become a portal into our lives in both physical and digital spaces--tying our online 'faces' to our physical ones. Significantly, "this conversion from image data to information continues silently behind the lenses of surveillance equipment generally unseen by the surveillance subject" [9].

Research conducted primarily in the UK, but also in Australia and Canada, tells us that people generally have a high degree of acceptance for video surveillance. For example, public opinion surveys by media outlets consistently find high levels of citizen support for camera surveillance [5]. But these surveys are generally conducted after some significant security-related event where cameras have either played a role, or it is supposed they would have played a role had they been present [14]. More rigorously designed surveys conducted by social scientists tend to find slightly less support for camera surveillance, and show that the location of the surveillance [14], the demographic group to which the respondent belongs [7], [15], and even the ways in which questions are framed [7] affect the degree to which people are willing to support camera surveillance. These studies also find that although, on average, about one third of respondents will agree that camera surveillance is a privacy threat, for many of that 33% it is still seen as acceptable because of a perception that it might improve safety or security [27].

The video surveillance landscape in Canada differs somewhat from that of other jurisdictions where research has taken place, in that most Canadian surveillance cameras are not part of publicly supported infrastructures. Instead, the majority of cameras pointed at publicly accessible spaces are commercially run and operated. These commercial operators fall under the PIPEDA (Personal Information Protection and Electronic Documents Act) provisions for informing individuals about the nature of video surveillance, and the Office of the Privacy Commissioner of Canada has issued guidelines for organisations using surveillance cameras [20]. However, it seems as though there is little compliance with even the basic guidelines regarding notification about the purpose of surveillance or potential uses of the personal information collected [2].

When we consider all of these issues--rapidly evolving and increasingly potentially intrusive technologies, lack of public awareness, and organisational non-compliance with privacy guidelines-- in combination with the principle, expressed in the Office of the Privacy Commissioner of Canada's (OPC) Guidelines for Overt Video Surveillance [8], that individuals have "the right to lead their lives free from scrutiny", it raises some significant questions. The unmitigated growth of video surveillance, in both scope and nature, is encroaching on any form of reasonable control a data subject may have over their personal information. The use and possible linkage of visual personally identifiable information is an issue that should concern us all.

But does it? As researchers concerned with information policy in general and privacy in particular, we assume that these issues are significant, but **are individual Canadians concerned about the information captured by video surveillance**? People may not know what can be done with their captured visual images, or what their rights are in relation to personally identifiable information gathered by video surveillance systems. Similarly, Canadians' level of knowledge about current video surveillance capabilities, and the way the technology is developing in the near future, is unclear. As information researchers and privacy advocates we are working to understand the policy implications of contemporary and emerging 'intelligent' video surveillance, but what we do not know is whether Canadians care about these developments. Or more significantly, we do not know whether they have enough information to develop an informed opinion. Our ongoing project therefore seeks to establish more clearly the current degree of general knowledge Canadian citizens have about video surveillance technologies, their attitudes, and their understanding of relevant privacy regulations.

A. In Situ Interviewing

To find out what Canadians know about visual surveillance practices and technologies, we needed to ask them. Our research takes a small step in this direction of this larger goal, by exploring the opinions and concerns of citizens in one large Canadian urban centre. The first step of this project was to conduct semi-structured "man and woman on the street" interviews. The questions focused on determining what people know about the video surveillance activities that are capturing their personal visual information, asking what they think about public video surveillance, and determining what they know about their privacy rights regarding such surveillance. We sought to understand the extent to which people recognize visual information as personal information, and the degree to which they are informed, or care to be informed, about the practices relating to visual information collected via video monitoring.

To date we have conducted 156 interviews in various urban locations where the presence of private surveillance cameras focused on public space is somewhat obvious, either because the cameras are visible, there are notification signs posted, or a combination of both. These sites are in the vicinity of major intersections, public squares and community centres. It was our hope that by situating the conversations with participants in sites where the cameras can be seen and discussed as a concrete presence, people might be encouraged to think about and answer the questions.

We based our core questions broadly on the OPC's March 2008 Guidelines for Overt Video Surveillance in the Private Sector, modified to reflect our focus on the surveilled rather than the surveillers:

- Did you know that this organisation conducts video surveillance?
- Why do you think this organisation conducts video surveillance?

This research is funded by the Office of the Privacy Commissioner of Canada through their Contributions Program.

- Did you notice any signs or notices that video surveillance is taking place?
- What do you think the organisation does with the visual images of you and others that it collects? What should they do with them?
- Does it concern you that you are being recorded? If yes, what are those concerns? If no, why do you feel comfortable with it?
- Would you ever want to access video information about yourself? How might you try to do that?
- Do you think video surveillance benefits you as a [shopper/citizen/member of the public]?

B. Findings

Our interview participants are Canadian citizens who range in age from 19 to 65, with education levels from high school level up to post-graduate degrees. They are engaged in a variety of occupations including law enforcement, education, child-care, engineering, construction and sales. While our participants represent a range of socioeconomic and demographic categories, our sample was not representative of all Canadians, nor does our data allow for a subtle examination of the effects that personal life histories, such as differing home countries or length of time as Canadian citizens, might have on individual perspectives about surveillance. Rather, it is a snapshot of the opinions of those individuals willing to speak briefly with our interviewers in a particular Canadian city. Further research of greater breadth and depth, reflecting other geographic areas in both urban and rural settings would be required to truly reflect a more representative Canadian perspective.

Our findings fall broadly into three categories: general awareness and perceptions of video surveillance; knowledge and opinion of privacy regulation relating to video surveillance, and information needs regarding video surveillance.

1) General awareness and perceptions of surveillance

When asked, the majority of our participants told us that they are aware that they are often under camera surveillance when going about their daily business in public spaces. They know that their actions might be caught on a camera when walking through a mall or even down a street. When asked why they think organisations are using video surveillance, most state that they don't know the specific purpose beyond a general perception of its use "for safety" or "for security and stuff." When we query what participants mean by the concept of safety in relation to video surveillance, it usually has to do with their perception that having cameras equates to someone watching, and this leads to an assumption that in surveilled areas, crimes are less likely to happen to them personally. As one participant put it, "I think it stops people from doing bad things, I mean someone is watching you and you can tell there's going to be consequences." This kind of assumption is potentially problematic for citizens, however. We know from other's research that cameras have not proven particularly effective at deterring crime, so it is not necessarily a valid assumption that it will, in fact, "stop people from doing bad things" (see for example, [10], [8]).

Comments such as this also indicate that it is generally not clear to citizens whether cameras are monitored live; in fact, in many locations, no one may actually be watching at any given moment, and some locations have no live monitoring at all. Sometimes participants coupled their belief that someone was watching live with the possibly erroneous expectation that if trouble occurs, help will be dispatched: "if something happens to me, I assume there is someone at the other end of the camera looking at things and is willing to send help if needed." When asked explicitly, do cameras in the area make you feel safer, participants had varying opinions ranging from "What is a camera going to do if I get mugged?" to "I feel indifferent" to "if something is being recorded I feel safe knowing someone will or is able to see what will occur." More than half of the people asked, however, stated they felt safer in the presence of video surveillance.

Participants also talked about the use of cameras for security, and by this it seems they meant the use of surveillance footage, after the fact, in order to investigate crime, identify, and then prosecute criminals. Most thought that cameras were useful for this purpose and were also generally supportive of privately collected information being given to police, although they were more divided when asked whether a warrant should be required to obtain this information. Participants were similarly divided in their perceptions about the personal benefit they might receive from video surveillance, but were somewhat unified in the opinion that there was some public benefit. As one person stated, "if that video surveillance helps the police or companies to apprehend criminals then I think that benefits me."

2) Knowledge and opinion of privacy regulation

When we asked people questions about their knowledge of privacy regulation for video surveillance, we found an interesting result. Relatively few participants stated that they knew that there were privacy regulations relating to video surveillance, and even fewer knew what those regulations were. However, almost everyone asked stated that they felt this kind of surveillance should be covered by regulation, and many said they assumed that it was. Participants generally said they wished to know whether an organisation was compliant with privacy regulation, and some also wished to know if an organisation had ever had a complaint filed against them or had been found in violation of privacy obligations.

The primary means by which organisations inform citizens about the presence of video surveillance is by posting signs, so we asked our participants if they had noticed signs about the video surveillance in the areas where interviews took place. Relatively few had noticed signs in our interview locations, but many mentioned seeing signs on commercial premises when they entered are being monitored by video camera "for [their] safety" or possibly "for theft prevention." Most of those asked believed signs were the appropriate means to inform them about the presence of surveillance, although some were critical of the content and visibility of signs they had seen in the past. Some participants specifically mentioned issues with signage location and size--"I have seen small miniscule signs under those set of stairs"-- and others describe the content as "incredibly vague."

In general, although there was a lack of information about the existence and nature of privacy regulation around video surveillance, there was a clear agreement among participants that this kind of surveillance should be regulated, and that it is important for organisations to comply with whatever privacy regulation might exist.

3) Information needs and wants

If asked specifically what they might like to know about camera surveillance and the way it is carried out or regulated, most participants said that they want to know that surveillance is taking place, "what area is under surveillance" and "what their reasoning was" for conducting the surveillance. There was some interest also in knowing more about specific organisational policies around surveillance, particularly in terms of retention policies--how images were stored, how long they were kept, and who had access to their personal information. A smaller proportion of participants were also interested in knowing how to contact the owner or operator of the surveillance cameras.

There was also a clear sense of what might be legitimate uses of surveillance data, such as use in identifying a thief, and what participants felt were illegitimate uses. In particular, participants were often uncomfortable with the idea that surveillance cameras might be used for customer tracking or profiling in retail outlets, or for citizen profiling more generally in public settings. All agreed that they would like to know if they were subject to surveillance for the purpose of these kinds of social sorting activities.

While our findings are limited in generalizability by our small sample size and single city site, some themes did emerge from our interviews. Our findings point to a need for public education around the ways camera surveillance is used, and can be used, what it is good at and what it cannot do, and about the current set of laws and regulations that provide citizens with rights to their personal visual information. Future fieldwork will include a series of workshops that will confirm our interview findings and allow us to engage in more in-depth discussion with participants around some of these key issues. We also are planning a public forum to contribute to public knowledge about these issues. In an ongoing and iterative fashion, the information we have learned from our participants about their opinions and information needs regarding video surveillance has also been used to inform our participatory design efforts. We will now turn to a discussion of the challenges, motivations, and rationale for designing the SurveillanceWatch application, and describe the prototype.

III. CROWD-SOURCING THE PUBLIC DISPLAY AND REMEDIATION OF PRIVACY NON-COMPLIANCE

A. The challenge of private sector privacy non-compliance and public ignorance

The troubling disjunction between widespread privacy non-compliance of private sector video surveillance operations [2] and the similarly widespread lack of knowledge among surveilled subjects who desire more information and greater legal compliance, poses a significant challenge for those concerned for civil liberties and information rights. What are the appropriate responses when the conventional mechanisms of liberal democratic governance have so far demonstrably failed?

Canadian privacy law as applied to the private sector is unusual in being based originally on an attempt at self-regulation. The Canadian Standards Association (CSA) in 1996 issued its Model Code for the Protection of Personal Information following a consensus process with strong industry involvement. In part reflecting the subsequent lack of voluntary adoption, the Model Code's 10 principles of fair information practice were incorporated verbatim in the Personal Information Protection and Electronics Documents Act (PIPEDA), the federal privacy legislation that has regulated personal information handling in commercial activities since 2000. Even with the force of law, compliance is weak. Canada's Privacy Commissioners are charged with enforcing the law, but because it follows a complaint based model, it requires citizens to file a formal complaint against specific alleged violators, which involves a protracted process that few people know about and even fewer are willing to pursue except in exceptional cases. The federal Privacy Commissioner's office can conduct independent audits, but its resources are stretched thin and it is generally regarded as 'toothless' - it can't write binding orders nor impose fines. Even when companies are found at fault, they can appeal to the courts and in any case there are no financial penalties. The news media, and investigative journalism in particular, are also regarded as having an important role to play in informing citizens and holding powerful institutions to account, but beyond frequent reporting of data breaches and other scandals *du jour,* do little to provide sustained and systematic coverage of privacy threats and remedies.

B. Rationale for a crowdsourced, counter surveillance approach to public accountability: documenting (non)compliance

While few argue for abandoning the legal apparatus, arms-length regulatory bodies and an independent media for correcting the shortcomings of contemporary governance, in the area of video surveillance these conventional mechanisms alone are clearly inadequate to the task of protecting the public interest. Indeed, this is recognized as a widespread characteristic of the prevailing neoliberal political/economic order [13]. One form of increasingly popular response to this perceived crisis of liberal democratic governance that takes advantage of the growing ubiquity of digital 'social' media is citizens individually and in ad hoc networks taking on the tasks of holding powerful organizations to account [1].

Given the importance of surveillance in the exercise of power, an appealing accountability tactic is that of 'counter-surveillance', which Gary Marx characterizes as a form of "surveillance neutralization" involving "role reversal as subjects apply the tactics to agents taking advantage of the double edged potential of tools" [17]. However, this form of surveillance often eschews the covert aspects of conventional surveillance that are seen as especially problematic. In conducting their surveillance openly and transparently "…counter-surveillance tacticians seek to disrupt…trends in the privatization, sanitation, and elimination of that which is 'public'" [18].

As we will see next, counter-surveillance often begins with the basic act of documenting surveillance operations, thereby drawing attention to their presence.

C. Other examples of crowdsourced, counter surveillance app-based public accountability tools

Counter-surveillance tactics such as reversing the photographic gaze, performance art, and installation mapping have been used by artists, activists and academics to publicly 'out' or reveal video surveillance for a number of years. For his "Shooting Back" video project, Steve Mann questioned front-line staff about the surveillance practices of their places of work, then confronted them with his own video camera [16]. The Surveillance Camera Players in New York City, founded in 1996, stage public performances directed at surveillance cameras [23]. These performances acknowledge and highlight the security apparatus and often engender a very public physical intervention from security personnel [18]. Also in New York, the Institute for Applied Autonomy's iSee project is a web-based application which allows users to map out a "path of least surveillance" [11] based on a database of known surveillance cameras in Manhattan. Another effort to publicize the presence of surveillance cameras occurred in Canada, prior to the 2010 Vancouver Olympics. The Vancouver Public Space Network (VPSN) and Simon Fraser University developed, with a team of volunteers, a map indicating the location of 1500 surveillance cameras in the city's downtown area [26].

More recently, the proliferation of mobile computing devices and small personal cameras has made crowdsourcing a viable approach to on-the-spot counter-surveillance, where members of the public are empowered and encouraged to report on events and issues that matter to them as they happen. Some current counter-surveillance resources include toolkits for documenting environmental concerns [21], monitoring police behaviour [19], and reporting on the state of public infrastructure [22]. Ushahidi, which emerged as a tool to track post-election violence in Kenya in 2008, has evolved into a platform which allows individuals and organizations to create their own crowdsourcing applications, with a focus on "democratizing information, increasing transparency, and lowering the barriers for individuals to share their stories" [25].[1]

SurveillanceWatch is inspired by the mapping and crowdsourcing approaches outlined above, but is distinctive in that it goes beyond simply drawing attention to the existence of surveillance cameras. We broaden the focus to video surveillance installations, including signage, ownership and regulatory compliance. In conjunction with this, we provide information about the prevailing legal requirements and how they apply to particular installations.

D. Aims and scope of the SurveillanceWatch app

The over-arching goal of the SurveillanceWatch project is to make video surveillance in the private sector and the related privacy issues more transparent, understandable and accountable to Canadians. In particular, the key objectives of the project include:

1 To increase public understanding of the extent and nature of video surveillance in their daily lives.

2 To document the extent of private sector video surveillance and privacy compliance in selected urban areas and industry sectors

3 To highlight the largest video surveillance owners/operators that are not compliant with privacy law, making them subject to public pressure

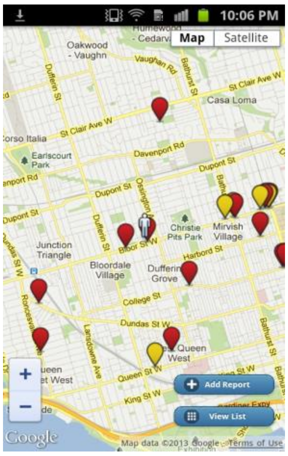
4 To highlight those video surveillance owners/operators who are most compliant with privacy law.

We seek to accomplish this by developing an easy to use smartphone app that interested individuals can use to take photos of cameras and signs of video surveillance installations, uploading these to a shared database with tags to indicate key privacy features of the installation. The app is designed to allow users to view the location and privacy compliance of installations in their immediate vicinity, or anywhere in the world.

E. The current prototype

The following section discusses design choices made to engage and empower citizens interested in video surveillance. SurveillanceWatch was originally conceived as an app for the Android Market. However, as we started development, we chose to also make it as a web application in order to reach a broader audience. The current version of SurveillanceWatch may be run as a native Android app, or it may be launched in a browser on computers and mobile devices.

The app makes it easy for a person to identify nearby video surveillance installations. The SurveillanceWatch home page shows a map displaying pins at the location of all known installations in the user's vicinity (see Figure 1).

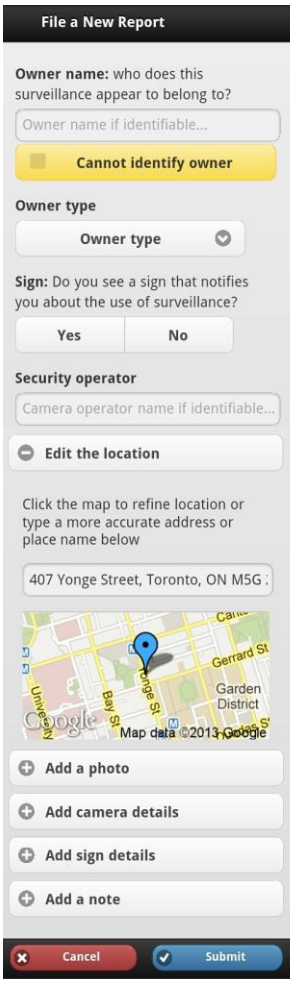


[1] Not all surveillance crowdsourcing is counter to established authorities. For example, the Department of Homeland Security's "See Something, Say Something" campaign [6] in effect crowdsources some policing functions to the public [24]. The iWatch app is a mobile application that may be deployed by local law enforcement agencies for the purpose of collecting information from the public [12].

Figure 1. Map View

The pins are colour coded to indicate their compliance (or non-compliance) with legal signage requirements - namely that video surveillance operators must post signage notifying passersby of the presence, nature, and scope of any surveillance installation they may be subject to. A red pin means that no sign was observed and that the installation is non-compliant with Canadian privacy regulation. A yellow pin indicates a sign was observed but that it was lacking information required for ‘minimal compliance’, while a green and yellow striped pin identifies installations that achieve ‘minimal compliance’ signage requirements. These requirements include high visibility, a clear indication of the installation’s owner and operator, a description of why the area is being surveilled, and a description of the installation’s properties - whether images are monitored or recorded, contact information for the individual responsible for protecting personal information captured by the cameras, as well as a reference to the legislation that governs the handling of this information. Finally, a green pin is reserved for installations that go significantly beyond the minimum necessary and demonstrate compliance with the ‘spirit’ of Canadian privacy regulations. The colour coding aims to provide the user with a sophisticated layering of information that is at the same time easy to access and understand.

When an individual notices a video surveillance installation that is not already represented in SurveillanceWatch, she may launch the app and add a new ‘report’ - thereby engaging in an act of counter-surveillance (Figure 2).



File a New Report

Owner name: who does this surveillance appear to belong to?

Owner name if identifiable...

□ Cannot identify owner

Owner type

Owner type

Sign: Do you see a sign that notifies you about the use of surveillance?

Yes No

Security operator

Camera operator name if identifiable...

Edit the location

Click the map to refine location or type a more accurate address or place name below

407 Yonge Street, Toronto, ON M5G

Add a photo

Add camera details

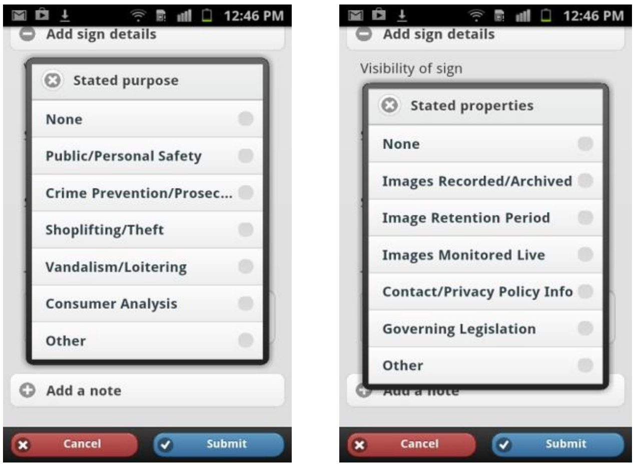
Add sign details

Add a note

Cancel Submit

Figure 2. Report Screen

Each report includes a name and description of the installation’s owner, the location where the pin should be placed (an installation which has multiple cameras may in fact cover several hundred square metres), and whether or not a surveillance notification sign was clearly visible. Users may also upload photographs of the site, report on the number of cameras they have counted for this installation, describe the spaces those cameras are pointed at (e.g. whether they are pointed at the interior or exterior of a building), and log a variety of characteristics of the notification sign (if one exists), such as its relative visibility, its stated purpose and properties, and the text of the sign (Figure 3).



12:46 PM

Add sign details

Stated purpose

- None ○
- Public/Personal Safety ○
- Crime Prevention/Prosec... ○
- Shoplifting/Theft ○
- Vandalism/Loitering ○
- Consumer Analysis ○
- Other ○

Add a note

Cancel Submit

12:46 PM

Add sign details

Visibility of sign

Stated properties

- None ○
- Images Recorded/Archived ○
- Image Retention Period ○
- Images Monitored Live ○
- Contact/Privacy Policy Info ○
- Governing Legislation ○
- Other ○

Add a note

Cancel Submit

Figure 3. Documenting the Purpose(s) and Properties of Surveillance

The use of a map as the application’s core grants individuals insight into the ubiquity of video surveillance cameras in certain public spaces. For example, the SurveillanceWatch map reveals six video surveillance installations (and seven unique cameras, as one of the installations has two cameras) covering a 150m stretch of Bloor St. West in Toronto (from Walmer Road to Spadina Road) (Figure 4).

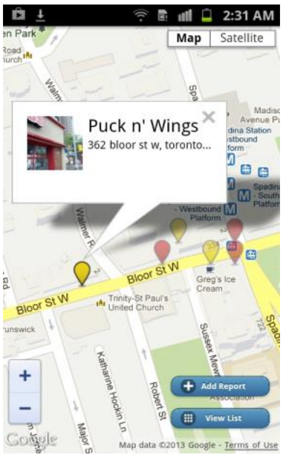
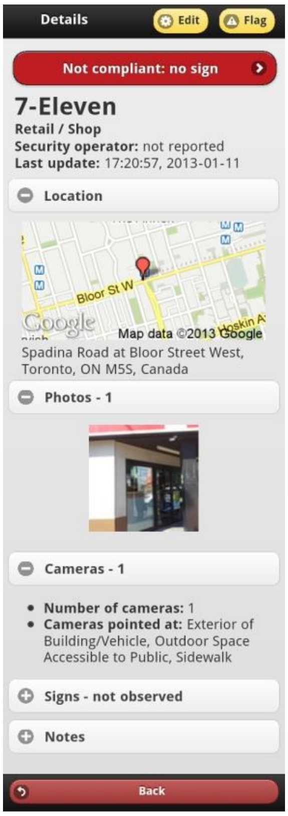


Figure 4. Cameras on Bloor St. West in Toronto

All seven of the cameras are pointed at outdoor space, and four of them are pointed directly at the sidewalk. This area sees substantial pedestrian traffic and many hundreds of individuals may have their personal information captured by these installations every day. As three of these installations exhibited no signage, and the cameras are relatively unobtrusive, the majority of passersby are likely not aware that they are within range of some of these video surveillance cameras.

If a user wishes to learn more about the video surveillance installations revealed through the SurveillanceWatch interface, she may access more detail by tapping on the installation's pin and then on the owner's name (Figure 5).



Not compliant: no sign

7-Eleven

Retail / Shop

Security operator: not reported

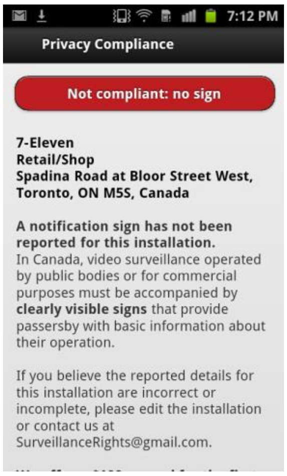
Last update: 17:20:57, 2013-01-11

Spadina Road at Bloor Street West,
Toronto, ON M5S, Canada

- **Number of cameras:** 1
- **Cameras pointed at:** Exterior of Building/Vehicle, Outdoor Space Accessible to Public, Sidewalk

Figure 5. Details Screen

If she notices any missing or inaccurate information she may edit the installation's details. This 'Details' screen is also a launch point for further information about 'compliance', such as how it is evaluated and assigned (Figure 6).



Not compliant: no sign

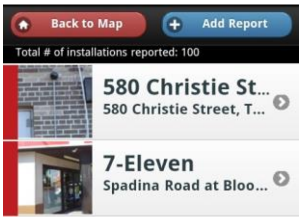
7-Eleven
Retail/Shop
Spadina Road at Bloor Street West,
Toronto, ON M5S, Canada

A notification sign has not been reported for this installation.
In Canada, video surveillance operated by public bodies or for commercial purposes must be accompanied by **clearly visible signs** that provide passersby with basic information about their operation.

If you believe the reported details for this installation are incorrect or incomplete, please edit the installation or contact us at SurveillanceRights@gmail.com.

Figure 6. Details about Compliance

Finally, the SurveillanceWatch 'list view' provides users with an alternate view of the data. This is sorted by Owner Name and thus allows individuals to browse for a particular Owner, or to quickly compare different implementations of a chain or franchise. For example, does one coffee shop have a better privacy record than another one down the street, and might this sort of knowledge impact consumer decision making? (Figure 7).



Total # of installations reported: 100

580 Christie St...
580 Christie Street, T...

7-Eleven
Spadina Road at Bloo...

Figure 7. List View

F. *Preliminary Observations: the prototype in use*

Even though the app is still being developed, and we have not attempted to 'launch' it in any concerted way, it is already attracting media coverage and public attention. The mobile app has had 1560 person visits, and the website has attracted 2386 unique visits. The database of user-generated entries is beginning to be populated, with 158 installations documented thus far. From the reaction so far by journalists and users, we can see that we are touching on issues of concern to people, and that they are gaining awareness of the extent of video surveillance, how it affects them and what rights they have.

One potential issue that may arise for individuals using the app in the public sphere is that, in our increasingly security-conscious society, institutions and organisations are often protective about the nature of their surveillance systems. Members of the research team have found that taking pictures of surveillance cameras in some settings is strongly discouraged by organisational staff or security personnel, and citizens using the app are likely to have similar experiences. There may also be the possibility, particularly at times when concern over terrorism is elevated, that users who are recorded by the cameras they are photographing might experience consequences if their actions are deemed suspicious by those monitoring the surveillance data. We do not know the degree to which users might consider these possibilities or be deterred from using the app. Another potential concern that users might have is the degree to which the app itself is privacy compliant. Users can access the app's privacy policy as the first item in the menu from the opening screen. As the app is part of a University project, the Ontario Freedom of Information and Protection of Privacy Act (FIPPA) applies, and our information collection practices are based on that Act. One potential issue that has emerged in the beta is that, while corporate names and addresses are considered public information as per section 2.3 of the Act, we have also had a small number of submissions regarding private citizen's home cameras. Ways to discourage the submission of this information and to prevent it from appearing in the application are being developed.

Despite these potential user concerns, however, we anticipate that as the app becomes further known, and the database of installations grows, that it will be a resource for users wanting to learn more the surveillance around them. It is our hope it may also be useful to researchers and policymakers seeking a deeper understanding of the extent and social implications of video surveillance as it is increasingly woven into the fabric of contemporary urban life.

Although the project's focus is on Canadian privacy legislation, we have received submissions from the U.K., the Netherlands, Portugal, Morocco, India, Malaysia, Australia, and from across the United States. While all pins in the app are colour coded based on the Canadian guidelines outlined above, a substantial international data set could reveal interesting patterns in the transparency and accountability of video surveillance operations internationally.

IV. Conclusions: Awareness, Consent, Compliance and Accountability

Our projects combine citizen-perspective focused research, participatory design, and public education in the expanding arena of visual surveillance and consumer privacy. We have two interlocking goals: to find out what people understand about the recent developments in video surveillance associated with the introduction of digital techniques, what concerns they express, and where information gaps exist; and to develop tools to help them assert their privacy rights and constructively engage with the surveilling organizations, processes and policies of video surveillance.

Our approach to measuring and raising awareness is multi-pronged, accomplished through our qualitative fieldwork, our app and our website. We have found that generally people are aware that they are often under surveillance in public spaces, but often unaware of the policies or regulations that govern that surveillance. They want to know, however, what is happening to their data in terms of retention and access. The SurveillanceWatch app takes these information needs into account, and allows users to document as many features of the surveillance installations they come across in their daily lives as are relevant to them. We hope that using the app generates awareness both of the presence of surveillance and a questioning attitude towards the way it is used and the degree of compliance with privacy regulation that organizations demonstrate.

Our fieldwork participants were clear that in most cases they would like to know if organizations collecting their personal data through video surveillance were compliant with privacy regulation. However, as we have noted, so far no reported private sector installation meets the minimum compliance standard for informative signage [2]. In the hope that increased citizen awareness can help encourage organizations to meet their privacy obligations, the SurveillanceWatch app allows uses to document the degree to which installations they see are compliant with privacy standards, and presents this information in an easily accessible and interpretable form. As signage is the primary means by which organizations notify people about surveillance, and notification is necessary for consent, the app allows detailed documenting of the information on such signs. Since informed consent is impossible if people are not given the chance to understand the nature of the surveillance before they enter the surveilled space, it is important that organisations take their responsibility to provide compliant signage seriously. The app crowdsources the assessment of compliance and renders that compliance visible.

This research is conducted on the assumption that the purposes of surveillance and the potential uses of visual surveillance data need to be made more transparent, and organisations using these technologies need to be more accountable to members of the public in protecting privacy rights. Accountability is multi-faceted and inheres with both organisations who collect data, and citizens whose data is collected. Organisations have a responsibility to develop clear policies and are accountable for demonstrating that they are compliant with the laws and regulations governing their surveillance activities. Citizens, in turn, have both the right and the responsibility to engage with surveillance policy at all levels, and we hope through the development and promotion of our SurveillanceWatch tool that we can help to make the importance of this engagement obvious and the process easy.

We are at a critical juncture in the development and deployment of video surveillance technologies. Their use and capabilities are increasing, while policies, procedures, and uses for the information that is visually captured for analysis are still evolving. This period of change and flux, when policy is malleable to disruptions and interventions is the ideal time for the development and deployment of privacy-protective measures to regulate the use of these technologies in the interests of civic safety and well-being. This is unlikely to happen, however, if Canadians are unaware of what is at stake. By finding out what they need to know and attempting, through technological mediation, to supply that information, we hope to help raise awareness and equalize some of the power asymmetries between surveillers and surveilled.

References

[1] Amnesty International, "Amnesty International report 2011: The state of the world's human rights, 2011. Available: https://www.amnesty.org/en/library/info/POL10/001/2011/en

[2] A. Clement, J. Ferenbok, R. Dehghan, L. Kaminker, and S. Kanev. (2012).” Private Sector Video Surveillance in Toronto: Not Privacy Compliant!,” in Proceedings of the 2012 iConference, 2012, pp. 354-362.

[3] A. Clement and J. Ferenbok, “Mitigating Asymmetric Visibilities: Towards a CCTV Signage Code,” in Eyes Everywhere: The Global Growth of Camera Surveillance, A. Doyle, R. Lippert, and D. Lyon, Eds. New York: Routledge, 2012, pp. 309-332.

[4] CSA - Canadian Standards Association, Model Code for the Protection of Personal Information (Q830-96), March 2006. Available: http://www.csa.ca/cm/ca/en/privacy-code

[5] W. Deisman, P. Derby, A. Doyle, S. Leman-Langlois, R. Lippert, D. Lyon, et al. A Report on Camera Surveillance in Canada (Part One). Kingston: Queen's University, January 2009. Available: http://www.sscqueens.org/projects/scan

[6] Department of Homeland Security, “If you see something, say something” campaign, n.d. Available: . http://www.dhs.gov/if-you-see-something-say-something-campaign

[7] J. Ditton (2000). “Crime and the city: Public attitudes towards open-street CCTV in Glasgow,” British Journal of Criminology, vol. 40, no. 4, pp. 692-709, 2000.

[8] A.. Doyle, R. Lippert, and D. Lyon, “Introduction,” in Eyes Everywhere: The Global Growth of Camera Surveillance, A. Doyle, R. Lippert, and D. Lyon, Eds. New York: Routledge, 2012, pp. 1-20.

[9] J. Ferenbok and A. Clement, “Hidden changes: from CCTV to ‘smart’ video surveillance,” in Eyes Everywhere: The Global Growth of Camera Surveillance, A. Doyle, R. Lippert, and D. Lyon, Eds. New York: Routledge, 2012, pp. 218-234.

[10] M. Gill and A. Spriggs, 2005. Assessing the impact of CCTV: Home office research study 292. [Online]. Available: https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf

[11] Institute for Applied Autonomy (IAA), n.d.. iSee [Online]. Available: http://www.appliedautonomy.com/isee.html

[12] iThinkQware, 2012. iWatch Mobile Applications [Online]. Available: http://ithinqware.com/icapture.php

[13] B. Jessop, “Neo-Liberalism,” in The Blackwell-Wiley Encyclopedia of Globalization, G. Ritzer, Ed. Chichester: Wiley Blackwell, 2012, pp. 1513-1521.

[14] S. Leman-Langlois, ” Public Perceptions of Camera Surveillance,” in W. Deisman, P. Derby, A. Doyle, S. Leman-Langlois, R. Lippert, D. Lyon, et al. A Report on Camera Surveillance in Canada (Part One). Kingston: Queen's University, January 2009, pp. 41-52.. Available: http://www.sscqueens.org/projects/scan

[15] S. Leman-Langlois, “The local impact of police video surveillance on the social construction of security,” in Technocrime: Technology, Crime and Social Control, S. Leman-Langlois, Ed. Cullompton: Willan, 2008, pp. 27-45.

[16] S. Mann, 1997. Shooting Back. Available: http://www.eyetap.org/wearcam/shootingback/

[17] G. T. Marx, “A tack in the shoe and taking off the shoe: neutralization and counter-neutralization dynamics,” Surveillance & Society, vol. 6, no. 3, pp. 294-306, 2009.

[18] T. Monahan, “Counter-surveillance as political intervention?” Social Semiotics vol. 16, no. 4, pp. 515-534, 2006.

[19] New York Civil Liberties Union (NYCLU) (n.d.). Stop and Frisk Watch App. [Online]. Available: http://www.nyclu.org/app

[20] Office of the Privacy Commissioner of Canada, 2008. “Guidelines for Overt Video Surveillance in the Private Sector.” [Online]. Available: http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp

[21] Public Lab, n.d. “Public Laboratory for Open Technology and Science - Home page.” Available: http://publiclaboratory.org/home

[22] Road Damage Assessment System (RODAS), n.d.” Rodas: track and fix potholes.” [Online]. Available: http://www.rodasproject.org

[23] Surveillance Camera Players (SCP), 2006. “Surveillance camera players: 10-year report.” [Online]. Available: http://www.notbored.org/10-year-report.html

[24] Tewksbury, D. (2012). Crowdsourcing homeland security: the Texas Virtual BorderWatch and participatory citizenship. Surveillance & Society, 10(3/4), 249-262.

[25] Ushahidi, 2013. About us. [Online]. Available: http://www.ushahidi.com/about-us

[26] Vancouver Public Space Network (VPSN), 2009. VPSN surveillance map. [Online]. Available: http://vancouverpublicspace.ca/index.php?page=cctv

[27] H. Wells, T. Allard and P. Wilson, Crime and CCTV in Australia: Understanding the Relationship, Centre for Applied Psychology and Criminology, Bond University, Australia, 2006. [Online]. Available: http://epublications.bond.edu.au/hss_pubs/70/