What do Canadians know about their video/visual privacy?

Prepared By:

Joseph Ferenbok
Brenda McPhail
Roxanna Dehghan
Alex Cybulski
Andrew Clement

Final Report

July 15, 2013

Contents:

Contents

Purpose

The growth of video surveillance systems and their ongoing augmentation by biometric and smart surveillance algorithms has significant implications for the privacy of all Canadians. The growth of ICT networks and developments in biometric technologies, such as face recognition, expand the potential uses of video surveillance data and make it increasingly important for Canadians to know their personal information rights. The "Who is Watching You" Project has been conducted to determine Canadian's attitudes towards current video surveillance practices, to find out what they know about new technologies and practices that will soon be available, and to determine the information that citizens need to become more informed about their privacy rights, and more active in protecting them.

This has been accomplished through two iterative steps. First, through "person on the street" interviews in a major Canadian urban centre, the project has produced a snapshot picture of what Canadians know about video surveillance and their information rights. Second, workshops have been conducted, with more planned, in order to explore the findings in more depth and to determine where public education should be best targeted to produce maximum effect.

This research fills an existing knowledge gap, and will provide researchers, governments and industry a snapshot to inform future research and policy in the unique Canadian context. The project addresses the following key questions:

a. What do Canadians know about video surveillance policy, practices and technology?
b. What do Canadians know about the implications of current developments in video surveillance and video analysis technologies?
c. What are Canadian attitudes towards video surveillance policy and regulation in Canada?
d. What information do Canadians need to fill in the gaps in their knowledge?

Background and Motivation for the Research

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 or commercial interests.

The progression away from closed-circuit analog video to cloud monitoring and digital surveillance opens up the possibility that the visual image data collected might soon be turned into actionable information. Information collected by networked digital sensors facilitate the processing of visual information either in real time or retrospectively into information--information which can be mined digitally for unique events or individuals or for analysis in aggregate. 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--ubiquitously and in real-time. And this growth has not gone unnoticed by the private sector. Existing private sector infrastructures may be incrementally upgraded to have profound implications for the mining and collection of visual data. Video analytics become an incremental cost with a large potential payoff: to know more about the customer. As the OPC notes in their Guidelines for Overt Video Surveillance (2008), individuals have "the right to lead their lives free from scrutiny." However, as the "conversion from image data to information continues silently behind the lenses of surveillance equipment generally unseen by the surveillance subject" (Ferenbok & Clement 2012), any realistic control individuals have over their image data is rapidly diminishing.

Although the users of video surveillance are often well aware of these "behind the scenes" technological advancements, members of the public most often are not. This is hardly surprising; not only are the technologies new and esoteric, but they are also generally used as part of a security system. Operators of security systems tend to prefer their methods to be opaque. Therefore, the primary easily-accessible means that Canadian citizens have of hearing about

video surveillance is in the public press, where, as it will be discussed below, the portrayal is largely positive and focused on specific instances of crime detection or prosecution. However few people seem to appreciate the nuanced understanding that video data is increasingly becoming actionable digital information and that the images captured by surveillance cameras in publically accessible spaces constitute personal and personally identifiable information; and that custodians of this information are regulated and obligated to protect your privacy.

Literature: Public perception and Academic Findings

A great deal of the research into the use and effectiveness of video surveillance, and attitudes towards it comes from the UK, where CCTV cameras are ubiquitous (Norris 1999). However, recently the acknowledged ineffectiveness of CCTV surveillance at reducing violent crime has prompted the current government in the UK to pledge more regulation and a roll-back of CCTV cameras ("People get power to take CCTV abusers to court" 2011). In Canada the situation appears to be somewhat different (Ferenbok & Clement 2012). Most cameras have not been placed by 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 provisions for informing individuals about the nature of video surveillance, but the findings of ongoing Canadian research funded in part by the OPC (Clement et al. 2012) find that there is little to no compliance with even the most basic guidelines. Collection of peoples' personal information seems to be seen as a right of retailers without any stated purpose or usage limitations, despite privacy legislation to the contrary.

Public perception of video surveillance is primarily shaped by the grainy pictures of wanted criminals released on the evening news, and by stories crediting such pictures with helping to identify those individuals, leading to their arrests. In the media, most often, the coverage is of incidents during which CCTV cameras revealed shocking, generally criminal events and where the footage either helped or failed to help to solve criminal cases. Calls for more cameras and the occasional call to fix existing cameras also appear. Infrequently, an article questioning the

benefit of camera surveillance versus its cost appears, usually in relation to one of those stories where the footage failed to assist in a publicized investigation. The articles have titles like "'I wanted to go down fighting!' Hero gran chases away robbers armed with a meat cleaver" (Edwards 2012) or "Shop worker fights off robber with bottle of Toilet Duck" (Didymus 2012). Not only do these kinds of articles predominate news coverage, but they are consistent across a range of international news sources from China, India, the UK, various Scandinavian and European countries, Australia, Canada, and the US. It is clear in studying media reports not only that CCTV really has become a rather ubiquitous technology, but that the way that these cameras are discussed in the popular press, across this wide range of international boundaries and cultural divides, is remarkably similar. Cameras help prevent crime. Cameras help catch bad guys. The perpetrator might have gotten away with it if not for the cameras. If we want to stop criminals we need more cameras.

Against this tide of overwhelmingly positive popular press stands a body of academic research that is similarly uniform in tone and conclusions. But in stark contrast to the media stories, study after study finds that cameras probably don't prevent crime, and for various reasons ranging from poor camera positioning, lack of ongoing monitoring, mechanical failure, or lack of oversight and integration with community policing strategies, cameras can't always help catch the bad guys after the crime happens, either. Researchers for the British home office found that CCTV is much more complicated to install correctly and use effectively than those who use it often consider (https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf), while the 20 contributors to a special issue of the *Surveillance & Society* Journal provide a range of critical perspectives on a number of topics linked to CCTV (http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/CCTV). This is not to say that all the research says cameras are bad; just that the reality is much more nuanced and complicated than articles titled "Caught on CCTV: Horrifying moment…" (Anonymous 2012) suggests. Up to this point, however, academic research has had relatively little effect on use patterns or public perception (Greenberg &Hier 2009).

In fact, 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 (Deisman et al. 2009). 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 (Leman-Langlois 2009). 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 (Leman-Langlois 2009), the demographic group to which the respondent belongs (Ditton 2000;Leman-Langlois 2008), and even the ways in which questions are framed (Ditton 2000) 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(Wells, Allard & Wilson 2006).

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 (OPC 2008). 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 (Clement et al. 2012).

The Office of the Privacy Commissioner of Canada has expressed the principle, in their Guidelines for Overt Video Surveillance (OPC 2008), that individuals have "the right to lead their lives free from scrutiny." If this principle is to be upheld in Canadian society, the use and possible linkage of visual personally identifiable information is an issue that should concern us all. This makes the disconnect between popular opinion and academic data particularly troubling, and clearly points the way to the need for more public education on the issues that arise in connection with video surveillance technologies. We will now turn to the ways in which

the “Who’s Watching You?” project investigated Canadian’s knowledge and opinions about video surveillance.

Methods

Each component of this research project, the interviews, focus groups and public forum had their own protocols and unique approaches described below. All focused thematically on trying to understand ‘engagement’ with Canadians on issues of video surveillance.

Interviews

To find out what Canadians know about visual surveillance practices and technologies, we went out on the streets to ask them. 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.

We conducted 156 interviews in various locations in a major Canadian urban centre. Locations were chosen where the presence of private surveillance cameras focused on public space was somewhat obvious, either because the cameras were visible, there were 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.

Our interview participants are Canadian citizens who range in age from 19 to 74, 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.

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. We began with nine question sets including questions such as:

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

During interviewing, the question sets were iteratively refined over three stages in order to focus the study and saturate key data categories. All of the question sets are reproduced for this report in Appendix A.

These questions sets produced a range of responses, discussions and observations that were recorded and transcribed, then coded using HyperResearch, a qualitative data analysis program, to generate categories of responses. The categories were then further coded and analysed to produce our preliminary findings.

Workshops / focus groups

Following the interviews, the Project team planned what was anticipated to be a series of three workshops/focus groups in order to test and confirm the interview findings, and to determine and the kinds of educational materials or sources that participants would be likely to utilize and would find helpful. The workshop setting has the advantage of allowing for in-depth discussion and probing of an issue, with the potential for new information to emerge from participants' interactions.

Workshops were scheduled for February 8, March 13 and April 17, 2013. Unfortunately due to a blizzard of sufficient severity to shut down the University, the March workshop was cancelled. Participants for the first workshop groups were recruited online using relevant email lists and through posters in public areas. In the initial workshop, discussion questions based on the interview data were developed, and were chosen in order to allow the research team to explore key categories with participants in greater depth. A series of exercises and questions (see Appendix B) were used to engage participants and elicit discussion.

For the second workshop, a broader, more aggressive strategy was used to attract volunteers. Researchers utilized social media, connecting with academic networks, student bodies and public interest groups. Given our timetable, we began advertising for the second workshop a month in advance so that we would have time to attract a large audience, but ensure that the event was memorable in the calendar of participants, with a final week media blitz to remind existing volunteers and secure other interested parties. Particular emphasis was placed on broadcasting the message widely, rather than ensuring it permeated institutional systems. Twitter played an

effective role in this strategy by connecting our recruitment officer with student groups and organizations who could re-tweet and re-distribute our call for volunteers to discrete networks. In this respect, connecting with organizations and institutions with similar interests in a cordial fashion was a key strategy in ensuring our call for volunteers was received broadly. One of the most consistent strategies utilized direct messages to organizational twitter accounts, or contacting an institution to request a tweet about our event.

Social media was particularly useful for the event, because it provided a two-way system of communication for participants and organizers. Based on feedback from potential volunteers, our team decided to serve a meal with the workshop to compensate its three-hour length. Participants were also able to communicate dietary restrictions and desires. Accommodating participant request was likely part of the reason of the high turnout in the second round. Communication with volunteers also allowed our researchers address any preliminary questions or concerns a participant may have had regarding the workshop. This interaction proved an incredibly valuable take-a-way for the research team. An unintended side effect of our social media efforts was wider recognition by other academics in our field who noticed our dispersion through other social networks.

In addition to some of the same exercises and questions used for the first workshop, the second workshop also utilized different techniques to activate the participants and elicit more robust responses to video surveillance. These corrections were made to resolve some of the difficulties we encountered in trying to solicit participant opinion by simply surveying their attitudes. In this effort, the second workshop activity focused on engaging participants with video surveillance, public space and policy in a "critical making" exercise. Instead of having participants talk about surveillance abstractly or through anecdotes, the second activity asked the participants to "create" a public space which was under video surveillance and describe its design and their reasoning in the design process.

The activity was modestly structured: participants were encouraged to form teams and supplied with materials intended to guide their responses in a meaningful direction without leading them to a specific conclusion. The first item was a surveillance camera, each with a different

appearance and function. The second item was a picture of a publically accessible place where video surveillance is routinely implemented. Finally, the participants were supplied with poster paper and writing materials to collect and express their ideas.

After distributing the materials, we asked the participants to design a publically accessible space under video surveillance using the picture as a setting, describing its design, the function of the video camera, the purpose of the surveillance and potentially, the policy which would make video surveillance both useful and/or respect privacy of the public. The goal of this technique was to encourage participants to think about video surveillance holistically: through the operator or institution's perspective, through the technology of video surveillance and through the participant's own understanding or knowledge of surveillance and privacy. Perhaps most importantly, this activity allowed participants who did not know much about surveillance technology or policy to conceive video surveillance as an artifact, guided by context, politics and the limitations of technologies; in essence, the participants could be more focused on created grounded examples. These examples would not only be rooted in reality, but the process of designing this space would allow them to make issues of surveillance and privacy material instead of abstract policy issues or black-box technologies, typically off limits to civilians.

Public Forum

A Public Forum was held on Tuesday June 4, 2013 from 1:00-4:00 pm to discuss the findings from this research and encourage discussion on the topic of video surveillance. Building on the results of both the interview and workshop stages of the research, this forum brought together citizens and experts to explore a range of topics related to visual surveillance and visual information policy. The forum was advertised using email lists, social media and through various public outreach vehicles of the University of Toronto.It was conducted at the University of Toronto and in virtual space. It combined the presentation of the Who's Watching You? Project findings, a presentation by Dr. Ann Cavoukian, Information and Privacy Commissioner of Canada, revealing her most recent white paper entitled "Surveillance: Then and Now: Securing

Privacy in Public Spaces,"and a panel discussion at the University of Toronto with a Canada-wide internet broadcast.

Our panel included representation from academia, industry, civil society and government. The panelists were:

- l Prof. Lisa Austin, Faculty of Law, University of Toronto
- l Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario
- l Nathalie Des Rosiers, General Counsel, Canadian Civil Liberties Association
- l Vance Lockton, Senior Regional Analyst, Office of the Privacy Commissioner of Canada
- l John Wunderlich, Privacy and Security Consultant
- l Moderator: Prof. Andrew Clement, Faculty of Information, University of Toronto.

Panelists were asked prior to the Forum to come prepared to answer three questions:

- What is the most significant challenge or opportunity facing video surveillance in Canada?
- What should Canadians know about video surveillance practices and policy in Canada?
- How can we encourage a healthy public discourse about video surveillance
- in Canada?

Questions were addressed in sequence, and each panelist had approximately five minutes to answer the question for each round. Discussion time followed each completed round of responses, and included questions from the audience and conversation/questions amongst panel members.

The video record of this public Forum is available at
https://www.youtube.com/watch?v=kSQ32MqE5dE&feature=c4-feed-u
and featured clips are available at:
https://www.youtube.com/channel/UCtwpXI6SIjdstE8RFpASi1w?feature=watch

Findings

Participants

Our interview participants are Canadian citizens who range in age from 19 to 74. Although the education levels of our participants ranged from high school to postgraduate degrees, the majority of our participants had a bachelor's degree or higher. The participants were almost evenly split between men and women, and are engaged in a variety of occupations including law enforcement, education, child-care, engineering, construction and sales. Our findings are discussed below in relation to the key questions posed in the Project:

1. What do Canadians know about video surveillance policy, practices and technology?
2. What do Canadians know about the implications of current developments in video surveillance and video analysis technologies?
3. What are Canadian attitudes towards video surveillance policy and regulation in Canada?
4. What information do Canadians need to fill in the gaps in their knowledge?

Question One: What do Canadians know?

There is a very high degree of awareness that video surveillance often takes place in public spaces. In fact, the majority of our participants—approximately three quarters of those asked--told us that they are aware that they are often under camera surveillance when going about their daily business in public spaces. They knew that their actions might be caught on a camera when walking through a mall or even down a street or walking across a public square. The expectation of being surveilled in public was often expressed to us as not only a commonplace activity, but as something to be expected as the norm in a large urban centre. Perhaps that is why almost twice as many people thought that visual information is not personal information as those who thought it was and those who were not sure or thought it was conditionally private, combined. This is particularly problematic since Warren and Brandeis, in the Right to Privacy (1890) grounded much of the modern understanding to the 'right to be left alone', directly in response to the flood of visual information produced by intrusive photographic practices. If only a quarter of respondents understand personal information to include a person's visual image then any public discussion of video surveillance policy or regulation is from the onset lopsided.

One participant who was self-identified as comfortable with regulated surveillance had this to say: " culturally I think it has shifted our values, we expect to be monitored at all times, we are then surprised when a camera is not functioning as in it's not actually recording, it's there for the sake of being there." Not all participants were so sanguine about their perception that surveillance on the streets was ubiquitous however; as another participant said:

> I think sometimes video surveillance is bit much. Surveillance was meant, in my opinion, to deter people from wrong-doing, and it got worse over the years. Now you don't even have any idea you are being monitored. So in some ways I just don't go into areas that are heavily monitored unless I have to.

Awareness of purpose

An overwhelming majority of respondents wanted to know why or for what purpose a surveillance system was put in place, but a similar majority stated that they did not know the specific purpose(s) of the surveillance system in the areas where we conducted interviews, or in the city public spaces more generally. Many of these, however, were willing to guess about the reasons, or felt they had a general sense of the reason; this general sense was typically expressed as a perception of its use "for safety" or "for security and stuff." A significant finding was that when we queried what participants meant by the concept of safety in relation to video surveillance, it usually had to do with their perception that having cameras equates to someone watching. For example, one participant provided the following example: "if I'm in a parking lot and I knew beforehand that someone will be watching an area for 24 hours and that help would come I would feel incredibly reassured and incredibly safe."

With someone watching, those respondents who indicated they felt safer in the presence of video cameras seemed to assume that, in surveilled areas, crimes are less likely to happen to them personally. This assumption was routinely predicated on a belief that there could be a real-time system response in the case of criminal activity--this is in contrast with the predominant use of cameras as archival record for forensics and prosecution. 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, Gill &Spriggs 2005; Doyle, Lippert& Lyon 2012). A false sense of security maybe engendered by a lack of understanding of the purpose and functions of the surveillance systems.

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 as a forensic tool, referring to the use of surveillance footage, after the fact, in order to investigate crime, identify, and then prosecute criminals--video information as evidence. Most participants thought that cameras were useful as evidence of crime or wrong-doing and were also generally supportive of privately collected information being given to police for these purposes. Participants were more divided when asked whether a warrant should be required to obtain this information, as we will discuss under the heading of policy.

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.”

Video surveillance policy

Just as individuals who participated in our project expressed awareness about the presence of video surveillance but not its specific purpose, we found that there was a similar relationship in their knowledge of organisational video surveillance policies. Most of the interview subjects who were asked about their policy knowledge were fairly certain that organisations would have, or were supposed to have, policies in place around video surveillance, but a much smaller proportion were able to identify a specific policy or policies.

Retention

In particular, one policy area that stood out as an area of interest and concern for participants was that of data retention. When asked what organisations should do with surveillance records/data, people often assumed that visual data would be stored or archived for subsequent access in the

case of a reported incident. Some also expressed the opinion that they should be destroyed after a period of time. While most participants did not express an idea about the appropriate time period for records to be retained, those who did have an opinion generally suggested periods of weeks rather than months or years for such data storage. Most participants asked did not feel they needed to know the specific time period for data retention but at the same time, they did wish to be informed by an organisation that a responsible policy was in place.

Access

Linked to questions of retention are those of access. The issue of access to personal information collected by video surveillance cameras almost never arose unprompted by the interviewer. In part this may be due to the fact that many participants did not think of their image, recorded by a camera, as personal information. Half of those asked whether visual information was personal information thought it was not. Of the remaining 50%, roughly 25% thought it was personal information and 25% were undecided or uncertain, or thought it might be only under certain conditions, such as when it was linked to other information including a name. People also sometimes made a distinction between an image in a public place and a private place, with the private being more likely to be personal information. Of those who say it is not personal information, there seems to sometimes be an assumption that they cannot be identified from a visual image, or as one participant put it, "The camera doesn't know who I am, so there's no personal information being spread"; while it was outside the scope of the present study to probe the conditions under which participants might come to see visual information as personal, it would be interesting to determine if an increased knowledge of facial recognition or other such techniques might alter this view. Based on concerns expressed when asked about new technologies (see Question 3, below), we might speculate that more information about this type of technology would in fact alter people's perceptions.

Although participants did not raise the issue of access independently, those who were explicitly asked about their information needs in relation to access were somewhat interested in potentially having access to surveillance data of themselves. While few thought they would want access generally, and none had ever made an access request, more thought that there might be circumstances in which they would like access. One participant imagined a scenario in which he

might want to ask for a copy of his personal data: "Well, if for instance I was injured in a public place I may need evidence in order for a claim that I may make against someone else then I would go to the owner of the camera and ask for my image."

Access policy is, of course, not only about an individual's access to his or her own information, but about the possibility that others might obtain access. Participants were uniformly against unfettered public access to surveillance footage. At various points participants expressed concern that information about them might be used in inappropriate ways by others. For example, one person expressed concern that someone filming him for surveillance purposes might "upload my video onto YouTube for instance without my consent and that's a violation." However, there was more division of opinion when it came to issues of access to surveillance footage for the purpose of law enforcement. While, as discussed above, participants felt that video surveillance was often used, and was frequently useful, for the purpose of apprehending or prosecuting offenders caught on camera, opinion varied widely as to the appropriate way for police to gain access to privately held video surveillance data. While most people expressed the view that it was appropriate to share video surveillance with police in connection with a specific crime, or to search for a specific perpetrator, some expressed discomfort with the idea of general access for police without cause. One participant phrased it as follows:

> …they should have like probable cause or some sort of warrant or should be in relation to a specific incident like a store keeper has been robbed, and they want video of that incident. I don't think they should use it for any reasons beyond for like just fishing expeditions, or something like that.

There seemed to be a high degree of trust in officers of the law in Canada; a number of people expressed a conviction that police would only want to see video surveillance if they had a reason, and seemed to express an implicit trust that this reason would be valid and appropriate: "there are really good reasons for cops to get a video recording or for business to. I mean they are trying to protect and serve the public." Others expressed less faith that reasons for requesting access for surveillance data would always be valid, but overall the perception seemed to be that it was often appropriate for video surveillance data to be shared with law enforcement. As one participant stated, "Well as long as it's dealt with in a legal manner, I guess I'm fine about it." The issue of legality of access is addressed by questions about warrants. Of those asked, most participants

indicated that it would concern them to some degree if police were routinely given access to camera surveillance data without a warrant.

Notification of policy

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."

Perceptions of technology

In general, the citizens interviewed for this project had limited knowledge of current surveillance infrastructures or technologies. One interesting distinction that people seemed to make in their perceptions was a contextual difference between what they deemed was 'public' and 'private'. People tended to link images gathered in places they thought of as private as personal information. While images gathered in public spaces were linked less to personal information because of a pervasive assumption that they could not be identified or tracked by the visual image. We did not probe to see whether biometric technologies and algorithmic surveillance strategies enabled by face recognition technologies would change their opinions of the contextual nature of personally identifiable information, but this is clearly an area of research that needs to be developed.

Summary

Opinions Canadians we spoke with about video surveillance practices during the course of this research varied however there were some distinct trends. People had strong opinions about the use of video surveillance data for profiling and social sorting. People thought video surveillance should be regulated, but were generally unaware of the regulations themselves. People responded strongly around issues of purpose, safety and crime prosecution. People generally assumed video surveillance was useful and beneficial to them (even if not directly), but also were generally supportive of central oversight and regulation.

Question Two: What are Canadian attitudes towards policy & regulation?

Generally people seem to be aware of and comfortable with video surveillance in public spaces. Nearly double the respondents, for example stated that they did not feel their behaviour changed in the presence of cameras than those who said that they did behave differently. But assessing attitudes towards policy and regulation during the interview process proved somewhat difficult simply because so many of our participants knew very little about surveillance policy or its regulation. We iteratively adapted some of our questions to at the information needs participants had around surveillance policy and regulation. Although we saw a range of attitudes towards video surveillance practices in both the focus groups and the on-the-street interviews, there were some clear over arching themes. Key findings are that attitudes:

· are generally not informed by an understanding of rights or policy
· are strongly negative towards all forms of profiling, especially in domains outside of 'security';
· suggest a general acceptance of surveillance as an urban norm;
· review a strong belief that video surveillance is either regulated already or should be; and
· suggest understanding about why surveillance is being use is a central issue for a significant number of respondents.

More granular attitudes of respondents are outlined below.

Information needs about surveillance policy

While nearly half of the participants asked were unsure about whether there was regulation covering video surveillance in public spaces or believed that there should be regulation, very few actually had some knowledge of the regulations or their existence. Despite the clear indication that there is a clear lack of awareness on the part of the majority of the participants regarding the

state of video surveillance regulation, only a very small minority of those interviewed expressed the belief that there should be no regulation of video surveillance systems in Canada.

While there was a general perception amongst our participants that video surveillance was beneficial to the public, there was a clear corresponding expectation that it should be regulated to ensure that those benefits would accrue to them. Participants expressed several needs for more information concerning the information policies of surveilling organisations. Many of them suggested that they would like to know more about the way that information was stored and particularly how long it was retained. They also expressed an interest in knowing who would have access to it during the retention period, and for what purpose(s). Closely linked to their perceptions of safety in relation to monitoring, as discussed above, participants also wanted to know whether or not someone was watching live while they were being surveilled, and whether or not a live surveillance monitor would have the ability to dispatch help in the case of an emergency that was caught on camera.

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 also wanted to know whether an organisation was compliant with privacy regulation, and many also wished to know if an organisation had ever had a complaint filed against them with the OPC or had been found in violation of their privacy obligations. This suggests there may be a large gap between what citizens' think is important and their knowledge of existing regulations

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. Only about a quarter had noticed a sign and equally as many assumed there must be a sign but they had not seen it. However,

participants were generally in favour of organisations providing signs to notify them about the presence of surveillance. For example, one participant stated: "I understand it's for people's protection I don't think it has to be all the time. I don't know what's done with the footage. I would like to see more signs you are being monitored by a CCTV camera, I think that people should have the knowledge that to know they are being recorded." 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."

When asked directly whether participants had noticed signage for the cameras in the vicinity of the interview, more than half said they didn't seen signs in the current location; another quarter, hadn't seen any signs, but assumed there must be signs somewhere citing reasons like they had seen signs in the past; and just over one quarter of those interviewed mentioned having seen signs for video surveillance in the area. Of the participants who had seen signs in the area, several were critical of their content, size or location.

The situation with signage seems to suggest that the current system is not an effective mechanism of communicating information with citizens. This may be as a result of a number of factors: citizens may not be aware of or recognize the significance of currently posted signs; signs are lost among other urban noise; people don't appreciate the implications of what the signs mean; or signs are simply not well developed or designed for interaction and information dissemination.

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. Many respondents thought information about an

organization's video surveillance should be online, a smaller amount thought signs would be useful for providing this information. Some respondents thought the government should handle this information, or start a public awareness campaign. How to better design 'smart' signage for contextual-civic information dissemination is a broader research question for future research.

Information needs and wants in relation to surveillance policy

Participants seem to feel strongly that they should be informed of surveillance, but there seems to be little awareness that being informed of surveillance and its purposes is a legislated requirement. 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. One participant put it this way" "I think the signs should say if someone is monitoring the footage live and why there is a surveillance camera, sometimes it could be for safety sometimes it could be for theft protection I think the public has the right to know why there is a huge camera staring at me and for what purpose."

While many participants were interested in knowing who owns or operates camera surveillance, proportionately fewer wanted to know how to contact the camera owner or operator. There was some interest also in knowing more about specific organisational policies around surveillance, particularly in terms of recording and retention policies--whether images were being recorded or viewed live, 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. Some participants differentiated between their expectations of privacy for their images when collected in public spaces and in private spaces. This suggests a contextual integrity understanding of privacy--a more nuanced understanding of privacy that is contingent on, for example, location. This points to another observable trend in the data, that some participants acknowledge different expectations of privacy based on public and private distinctions. When it came to privacy, most people who commented directly on the issue were skeptical regarding surveillance practices and their ability to determine where there information goes. A vast majority of those interviewed wanted to know if an organization operating video surveillance was found in contravention of privacy laws. Of

these responses many used strong language: the word “absolutely” was often used to describe its necessity.

Very few respondents expressed any knowledge of their rights to access regarding video surveillance. Fewer still were interested to having access to their records, although several participants did acknowledge situations or contingencies where they saw the need to gain access to their information. For example, one respondent suggested access would be important as proof of an injury or crime. Another respondent felt strongly that only authorities should have access to video information and felt access might undermine the potential good of the system to prevent crime. A majority of respondents saw policy as an important factor in policing video surveillance. This concurs with the above discussion that a majority of respondents felt that the policy always needed oversight and a warrant to access video surveillance data.

Most respondents thought video surveillance is beneficial to them in at least one category of shopper, citizen or member of public, some felt the benefits were situational or contextual. About half the respondents who felt video surveillance felt it was beneficial because of safely, while the other half mentioned some form of security or policing including crime prevention, detection and prosecution.

Summary

While no respondents questioned the usefulness of video surveillance some questioned its use. All respondents thought the use of surveillance to provide immediate assistance was an appropriate use, some emphasized this point emphatically. A majority of responses indicated that individuals thought video surveillance should be used to detect crime. Consistent with other categories, a majority of responses thought that surveillance was used, or should be used to prevent crime. Responses regarding crime detection often conflated the implementation of surveillance with safety, by suggesting that it would be useful after-the-fact.

Of the respondents asked directly majority of respondents thought it was appropriate or good to use surveillance for security and deterrence. However, further analysis of these responses demonstrate that most individuals used both the term safety AND security. This might demonstrate that understandings of these concepts are poorly defined. Equivocation of safety and

security may demonstrate an uncertainty of what these concepts mean in a video surveillance context. One very certain and clear finding was that an overwhelming majority of respondents thought profiling was an inappropriate use of video surveillance. Profiling of any sort consistently met with strong disdain—suggesting that Canadians to have some strong attitudes about public profiling and sorting using video surveillance, when they are provided with the language and information with which to discuss the issues clearly.

Question Three:
What do Canadians know about video analytic technologies?

Video analytics is a technology capable of identifying and categorizing individuals subject to video surveillance based on their ableness, age, behavior, gender and identity; functions which are controlled by software which processes video and extracts this information. In this respect the technology of video analytics in incredibly powerful because it automates a process that was once the sole domain of human operators who manually sifted through video data with far less efficiency. Our study regarding this technology can be divided into two areas of interest. First, we wanted to gauge Canadian awareness of video analytics, in particular a popular application of this technology, facial recognition. The second area of focus for the study surveyed Canadian attitudes towards this technology, particularly how Canadians perceive its potential application and whether they would like to be informed of its implementation in public spaces. As the responses to these research areas indicate, Canadians do not know enough about video analysis technologies, but express a significant concern over its functionality when it is described to them in simple language. Among those interviewed, respondents specifically objected to the application of video analytics as a tool for profiling and social sorting in publically accessible spaces and wanted to be notified when it was implemented.

Awareness of Facial Recognition & Video Analytics

Facial recognition is undoubtedly the most popular application of video analytics; it appears in websites like Facebook, the viewfinders of digital cameras and on popular television shows with some frequency. In public spaces facial recognition is positioned to challenge civil liberties, identifying an individual as they pass through networks of video surveillance systems. Yet when Canadians were asked about facial recognition software, more than half of those interviewed in our study demonstrated limited to no understanding of the technology. Among those that did,

two identified facial recognition from their experiences with the popular applications listed above, while the remaining respondents correctly noted that facial recognition utilized a database for the purpose of comparing facial features. While a lack of awareness regarding facial recognition might be surprising given its proliferation in domestic life, it most likely signifies an inability to associate the name of the technology with existing practices, rather than total ignorance of its existence.

Much in the same way that respondents were unable to identify facial recognition as a technology they were familiar with, those interviewed fared similarly when questioned about their understanding of video analytics. Among our respondents, a vast majority had never heard of the technology and could not describe it in any meaningful way. Only two respondents surveyed during our study could confidently define video analytics and one of these respondents only learned of the technology because they looked it up after seeing a notice that our researcher would be conducting interviews on the topic. Given that identification of facial recognition was minimal it is perhaps unsurprising that respondents demonstrated even less awareness of its parent technology.

Serendipitously, one of our questions involving profiling did yield some interesting data regarding an individual's awareness of a video analytics system which they personally oversaw. While conducting interviews in First Canadian Place in Toronto, one of our researchers encountered an individual who worked in a senior position in a prominent hotel chain. During an exchange with the researcher, this individual acknowledged that: "we would like to keep certain people out [of the hotel], for example homeless, or deranged people. And it [the camera] monitors someone's gait, if it's slow and shuffled or strong and with a straight back." This quotation is significant not only because it identifies the existing application of video analytics, but it also confirms its use in discriminatory practices.

These results demonstrate that video analytics is a "black box" technology, with limited contemporary applications in consumer culture which might hint at its functionality. Without further public education regarding its application, video analytics is likely to remain a black box technology for some time. This lack of recognition supports many of the underlying recommendations made by this report, particularly the need for greater public education regarding the capacity of video surveillance.

Information Needs: Limitations, Use and Purpose

Providing information about video surveillance is the first step in addressing public education regarding the technological capacity of CCTV systems. Anticipating that those surveyed would have minimal knowledge of video analytics, our question framed its functionality in simple terms to determine if Canadians would like to be informed about its implementation. The question: "[Would you like to know] whether the video surveillance system was automatically analyzing your image to determine what type of person you are, specifically your age, gender, race or even your name?" identifies the concepts of video analytics, without discussing them in overly technical language. All of the respondents asked this question answered affirmatively, indicating a strong desire to be informed if video analytics were being employed in a specific area. This result indicates that the implementation of these technologies is a pervasive concern to the public, who should be informed of its location and implementation.

Attitudes

Similar to our question on information needs, our question regarding the use of video surveillance for profiling simplified an explanation of video analytics to account for its functionality without technical language. As a result, we asked those interviewed: "[Do you think it is appropriate for a video surveillance system] to determine what type of person you are (e.g. your age, gender, race, or even your name) to better apprehend or exclude those that the organization considers risky?" An overwhelmingly majority of respondents asked this question thought it was inappropriate for video surveillance systems to be used to profile and exclude individuals. In many cases, this question elicited a strong reaction from those interviewed, with many indicating that they were very uncomfortable with profiling as the premise of video surveillance. As one participant put it, "Good heavens! That is really something, can they really do that? Well for one I really want to know if they can do that, and two, if they are doing that they should stop" (Dundas Square, February 2013).

Advance Technologies

Ultimately, video analytics and advanced CCTV technologies were only a peripheral focus of this study on Canadian attitudes & knowledge of video surveillance and its practices. Despite

this limited focus on advanced technology, the response regarding video analytics demonstrated three lessons. First, our participants know little about the functionality of video analytics technology, even in popular applications (facial recognition) already used in existing consumer technologies. Secondly, when informed of its functionality people want to know when video analytics technology is employed in public spaces. Finally, participants expressed a mistrust of the technology and its application, particularly for private use in profiling and marketing. Many saw video analytics as an unjust application of video surveillance, expressing moral and social concern (if not disgust) regarding its implementation in public spaces.Many simply said that such a use for the technology was "inappropriate," but some spoke out more strongly: "who decides who's risky, am I risky because I'm black? Are you risky because you are student. No."

Despite the strength of the answers we received in our interviews and workshops regarding video analytics, these responses only form the beginning of an important conversation. The answers we received do not facilitate a nuanced understanding of attitudes towards this technology. First and foremost, questions asked regarding Canadians' knowledge of video analytics demonstrated a vast gulf in the power of this technology as compared to the average citizen's awareness of its capacity. Secondly our questions regarding the application of video analytics were limited by the scope of this study. In this way, the responses collected cannot be expected to encapsulate attitudes regarding an issue as complex as profiling mediated through the use of video technology. Undoubtedly some granularity must exist among Canadians regarding their attitudes towards the individuated features of video analytics and its potential application; certain responses gathered already reflect this diversity of opinion. Further study would provide avenues for understanding not only what functions under the umbrella of video analytics are palatable to the Canadian public, but also under what circumstances this technology might be leveraged in socially and morally acceptable ways.

As other data from this study has indicated, many respondents thought video surveillance should be used to provide assistance to those in need. It is worth noting that video analytics, particularly behavioral profiling, is tremendously promising in its potential to identify opportunities for care to those who are injured, lost or in need of other forms of assistance. In this respect, video analytics is not anathema to civil society, but further analysis of attitudes surrounding its implementation would provide a better understanding of how and when the technology should be employed in public space.

As the respondent from the hotel chain demonstrated, video analytics are already being employed to analyze individuals in high profile locations, where it augments existing security practices and its impact is minimal. Despite the small footprint of video analytics in current surveillance practices, its proliferation will undoubtedly increase as the cost for such technology decreases; Google Glass and digital signage are harbingers of the commercialization and expansion of video analytics. This potential for growth in this sector of surveillance technology stands in stark contrast to the attitudes of Canadians regarding the technology and their fear of it being used in profiling demonstrates an overwhelming mistrust of its potential application. While this dilemma is representative of many privacy issues surrounding new technologies, the relative immaturity of video analytics is fertile for both further study and public education regarding the application of the technology: to determine policy directions before the horse has left the stable.

Summary

In a society where wearable and ubiquitous video surveillance machinery are increasingly becoming the norm, it is disconcerting that Canadians know so little about the functionality of these technologies and the video analytics technologies that are increasingly driving our 'smart' devices. These technologies, like face-recognition technologies, are already in our cameras, on Facebook and in our cell phones, but most people do not seem to understand the extensive implications of their use(s). Of those participants who claimed some knowledge of these advances expressed a mistrust of the technology and its application, particularly for private use in profiling and marketing. The vast majority of others should be informed on the potentials of these technologies to participate democratically into their integration into political and socio-technical practices in our society.

Question Four: Do Canadians care?

It is probably safe to say that Canadians do care about the privacy implications of video surveillance technologies and how they will affect their lives. Once engaged in discussion, many participants had a range of topics they wanted to broach regarding video surveillance. But it quickly became overwhelmingly evident that most people do not have a core vocabulary or base understanding of Canadian policy or recent technological advancements to adequately engage with the debate. However, it was clear from our focus groups and street interviews that behind the relative silence--still waters run deep-- those we spoke with, generally 'cared' about some aspect of the implications of video surveillance.

Our data suggest that people are concerned with context of surveillance and are more comfortable in some situations than others. Although a high percentage of respondents felt comfortable with the presence of surveillance in public spaces, the majority of people felt either uncomfortable with the surveillance or felt that the issue was more nuanced, problematic and contextual than just putting up cameras. Almost a four-fifths majority of those interviewed wanted information provided about the owner or operator of a surveillance system. And a slim majority of respondents wanted to be notified, or thought it would be right to receive notification if subject to video surveillance. A slightly smaller number did not think this information needed to be provided. This suggests that respondents did care about issues around video surveillance but that 'care' encompassed both ends of the spectrum from perceived personal and social benefits of surveillance to those concerned with the implications to personal and social rights.

Our participants also clearly cared about the uses of surveillance. However, they did not 'care' uniformly. More Respondents reacted to concerns about profiling activities then express a general discomfort with recording or system related privacy concerns. Few respondents seemed to care enough about video surveillance to actively make different choices. One respondent said he had tried to resist video surveillance when he was younger and doing "stupid stuff" but doesn't anymore. That same person suggested that the cameras did not deter him from wrong

doing, just made him more careful. One person discussed resisting surveillance until he found it interfered too much with his everyday life, so he stopped. When asked about whether levels of surveillance should go up or down one person responded "I think more or less doesn't matter to me, what matters to me is why." What the Canadians we spoke with seemed to clearly care about were uses of their visual images for such purposes as social sorting and profiling.

As practice, policy and technologies of video surveillance change what seems to be consistent is that people care about how their visual data is used, for what purposes it is recorded or analysed and what benefits to do then (and society) derive from the surveillance. People generally support cameras for crime prosecution and crime reduction, but generally do not equate these outcomes with profiling, biometric identification, tracking and surveillance of the general population.

This gap, between what people what seem to want video surveillance to do (fight crime, prevent terror, improve safety) and what is required (e.g. video analytics and smart-automated-surveillance systems) for systems to accomplish these tasks is both a challenge for policy and regulation. Canadians deserve to be informed about how video surveillance systems are operated and regulated in order to make informed choices about future policy and regulation. Continuous ubiquitous video surveillance may soon change norms in private and public spaces, informing Canadians about the implications of these technologies is foundational to shaping current and future practices by an informed democratic populace.

Informing Canadians

We asked people what kind of things they would want to know about the video surveillance systems. Almost all respondents wanted to know if they were being recorded, in addition a few mentioned that they might want to know more information, like whom to contact or why they were being recorded. All respondents interviewed, said that they would like to know if assistance was available in an area under video surveillance. A vast majority of those interviewed wanted to know if an organization operating video surveillance was found in contravention of privacy laws. Of these responses a large amount used strong language: the word "absolutely" to describe its necessity. A majority of those asked wanted the information to contact the owner or operator of a surveillance system provided. A majority of

respondents would like to have information available on if surveillance cameras were being watched lived. A smaller majority wanted to know if their image was being recorded.

Many participants did not identify visual information as personally identifiable information. This is problematic when trying to understand what people think and know of their visual privacy because they lack the basic vocabulary and understandings of what constitutes personal information both according to PIPEDA and OPC guidelines. Until people understand that we are entering a time where our faces and other biometrics can serve as gateways into our public and private identities, people will unlikely to have enough information to understand the implications of video surveillance policy. The imminent launch of mainstream wearable computers that upload video to corporate servers while providing users a mediated vision experience, will undoubtedly challenge this norm. It is one thing to be observed from cameras up high, and another to be observed at eye-level while engaged in conversation with an individual face-to-face. As more people realize their images are being captured, broadcast and analysed, it is likely that their perspective on what constitutes personal data will change. Technologies like Google Glass, that steam and archive video information, may mean that every conversation, event, interaction and even a stroll down the sidewalk will produce traceable data that is both ubiquitous and surreptitious.

We set out to understand what Canadians think about video surveillance and its regulation and we have found to date, that there are several broad themes among our participants that have implications for future research, education and policy. We observed that:

- Most participants are aware of some form of video surveillance in public spaces;
- Some are aware of or have noticed signs about video surveillance but most think signage is an appropriate way to inform them about surveillance;
- Few are aware of any rights or regulations surrounding video surveillance information, though many assume they exist;
- Few understand the changing infrastructures, capabilities or information flows of networked digital video surveillance;
- Many interviewees expressed a desire to know the purpose for the information collection; and

- Most reactive negatively to any form of profiling or social sorting.

It would seem that few people know what may be done with their visual images. Fewer still are aware of their rights in relation to personally identifiable information gathered by video surveillance systems. And, most people we interviewed did not know or understand current video surveillance capabilities (much less appreciate the granularity of surveillance that video analytics may represent through image collection in private places through stationary and portable cameras). So, on the whole it would be safe to say that Canadians we interviewed do not have enough information to develop an informed opinion about video surveillance practices, regulation and technologies.

However, our participants did generally seem concerned with their visual privacy; and perhaps more significantly, many became engaged in conversations about the subject well beyond the scope of the framed questions and were interested enough to engage with researchers further. Canadians, at least those we spoke with, do care enough about the specific purposes behind the uses of video surveillance and would potentially be willing to engage if a more public discussion and debate were to be initiated. Canadians do care about their visual privacy--especially in reference to any form of automated public sorting or profiling of race, gender, age, or sex, but we found that many do not have the vocabulary, information or opportunities for public engagement on the subject.

Our findings clearly 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. With technologies that embed cameras into wearable accessories, bring video surveillance not only to street level but also to every wired user, peoples understanding and tolerance of the practices and regulation of these technologies is likely to become much more at the forefront of discussion and likely to change significantly over the next decade.

We will give one of our participants the final word: “security cameras are not being used properly and the regulation that mandated it are not being followed properly. I would like to see

more transparency in this ... this should be publicized more of a marketing campaign is needed. I hope this happens."

Closing Thoughts

This research has produced a snapshot of what people think about public video surveillance. There is no doubt that we are only seeing the very tip of the surveillance iceberg and will, as a society, face many new and unforeseen opportunities and challenges. Public and private video surveillance by individuals and institutions is not going to go away. As these technologies become completely pervasive and ubiquitous many choices and compromises will be made moving forward that will shape the society of our future. Flexible and responsive policy that works to protect the rights of individual to informational self-determination while balancing the needs for institutional monitoring is key to building a democratic Canada.

Opinions and attitudes we gathered, suggest that Canadians need more information about video surveillance practice and regulation to make informed contributions to policy. Along the way we have learned some very significant lessons about how people view video surveillance and how unaware people are of its potential. We have also noticed how social media may be used to countermand some of the effects of surveillance by mobilizing groups of people through political discussion and action. We discovered the potential for motivating people to participate and contribute to social research. Questions of who is watching whom AND why are only going to become more pervasive as networked surveillance media continues to become more ubiquitous. This suggests that, among other areas, more research needs to be done regarding how biometric and analytic technologies will change people's attitudes, practices and expectations of privacy.

References

Anonymous. (2012). "Caught on CCTV: Horrifying moment man pretends to be a 'Good Samaritan' as he leads a drunk woman to a taxi... before taking her home and raping her," Top News Today.org , November 12, 2012. Retrieved from: http://technology.topnewstoday.org/internet/article/3769490/

Cavoukian, A. (2013). Surveillance Then and Now: Securing Privacy in Public Spaces. Available: http://www.privacybydesign.ca/content/uploads/2013/06/pbd-surveillance.pdf

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

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

Didymus, J.T. (2012). "Video: Shop worker fights off robber with bottle of Toilet Duck." Digital Journal November 2, 2012, Retrieved from :http://www.digitaljournal.com/article/336027.

Ditton, J. (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.

Doyle, A., Lippert, R. & D. Lyon, (2012). "Introduction," in Eyes Everywhere: The Global Growth of Camera Surveillance, A. Doyle, R. Lippert, and D. Lyon, Eds. New York: Routledge, pp. 1-20.

Edwards, A. (2012). "I wanted to go down fighting: Hero gran chases away robbers armed with a meat cleaver," Mail Online, November 14, 2012, Retrieved from: http://www.dailymail.co.uk/news/article-2232640/Hero-gran-Trude-Mian-chases-away-robbers-armed-meat-cleaver.html.

Ferenbok, J. & A. Clement (2012). "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, pp. 218-234.

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

Greenberg, J. and S. Hier. (2009). "CCTV Surveillance and the Poverty of Media Discourse: A Content Analysis of Canadian Newspaper Coverage." Canadian Journal of Communications 34.3: 461-486.

Leman-Langlois, S. (2008), "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, pp. 27-45.

Leman-Langlois, S. (2009). " 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

Norris, C. & G. Armstrong (1999). The Maximum Surveillance Society: The Rise of CCTV. New York, Berg.

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

"People get power to take CCTV abusers to court - Telegraph." http://www.telegraph.co.uk/news/uknews/law-and-order/8317173/People-get-power-to-take-CCTV-abusers-to-court.html (Accessed March 13, 2011).

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

Appendix A: Question Sets

Pilot Interview Guide July 2012

Group one (general awareness)

- Did you know that this organization (where we are standing) operates surveillance cameras and likely captures images of you and other people?
- Why do you think this organization conducts video surveillance?
- Did you spot any signs or notices that video surveillance is taking place?
- What do you think the organization does with the visual images of you and others that it captures? What do you think they should do, or not do, with them?
- How do you feel knowing that you may be viewed by the camera operators or others with access? Are you comfortable or uncomfortable knowing that?
- Does having video surveillance in this area help you feel more or less safe?

Group two (legal uses)

- Did you know that this organization (where we are standing) operates surveillance cameras?
- How do you feel about being recorded? Are you comfortable with it or does it bother you?
- Businesses that use video surveillance cameras sometimes give their recordings to police or other law enforcement agencies. How do you feel about that?
    - (if participant expresses concerns) what specifically are you concerned about?
    - (if participant says they're ok) Why do you feel comfortable with it?

- Do you think the police should have a warrant approved by a judge before getting access to video surveillance that they don't operate themselves?
- To what degree would it concern you if police had access to video surveillance without a warrant approved by a judge? (Provide a range: Not at all; a little, definite concern; a major concern.)

Group three (privacy rights, knowledge)

- The organisation we're standing in front of uses video camera surveillance. Do you think that this video surveillance should be covered by Canadian privacy law and regulation?

- Do you know whether or not the surveillance operator is supposed to inform you about this video surveillance?

I'm going to read a list of things you might or might not want to know about the way this organisation conducts video surveillance; for each one, I'd like to know if you think it is something you absolutely want to know about, would like to know about, or don't want/need to know about:

  - who owns or operates the camera surveillance
  - the purposes for which they are operating the camera surveillance
  - how to contact the owner or operator
  - whether someone is watching live
  - whether help would come if you needed assistance
  - whether your image was being recorded
  - how long your images were kept before being deleted
  - who had access to your images and for what purposes
  - whether the video surveillance system was automatically analyzing your image to determine what type of person you are (eg your age, gender, race, or even your name
  - ---
  - whether privacy complaints had been filed against the organization
  - whether the organization had been found in violation of its privacy obligations, by the courts or the Privacy Commissioner

(Interviewer pick one of the items the participant answered "absolutely want to know" and ask why they feel strongly about that item) Why did you say that you absolutely want to know about X?

Group four (privacy rights, access to information)

- Did you know that this organization (where we are standing) operates surveillance cameras cameras and likely captures images of you and other people? ?
- Do you think of visual images--pictures or recordings of yourself—as personal information?
- Do you know whether or not you have a right to obtain access to the recording of yourself on camera?
- Would you ever want to access video information about yourself? How might you try to do that if you wanted to?
- Have you ever requested access to you personal video information? If so, what was the result?
-

Group five (compliance and value of video surveillance)

- Did you know that this organization (where we are standing) operates surveillance cameras?
- Would it concern you if the operator of this video surveillance is not compliant with Canadian privacy law?

- I'm not referring to this particular place, but many video surveillance operations don't completely follow Canadian privacy law. What do you think should be done about this?
- Do you think video surveillance benefits you as a [shopper/citizen/member of the public]? (if yes, how? If no, why not?)
- Do you think organisations should have to tell you more about why they use video surveillance and what they do with the information they collect about you?
- How could they do that in a way that would be helpful or interesting to you?

Group six (perceptions of surveillance)

- Did you know that this organization (where we are standing) operates surveillance cameras?
- Do you ever think about whether or not you're on camera when you walk around the city/mall?
- Do you behave differently if you know you're on camera?
- Did/do you avoid or resist the video surveillance system in any way? How?
- Would you like to see more, less or about the same amount of video surveillance? Why?
- Does having video surveillance in this area help you feel more or less safe?

Group seven (information needs)

- The organisation we're standing in front of uses video camera surveillance. If you wanted more information about their policies about video surveillance and privacy, where would you look?
- Should the organisation be responsible for communicating that information to you? How?
- Thinking more generally about video surveillance, where would you go or what would you do if you were interested in finding out information about video surveillance or your privacy rights?
- Who should be responsible for communicating or making sure that general information about video surveillance and privacy is accessible to you if you want to learn about it?
- How important do you think it is to make sure organisations are obeying privacy law when they conduct video surveillance? 1-5 scale, with one being very important and 5 not important at all.

Group eight (knowledge about infrastructure)

- Did you know that this organization (where we are standing) operates surveillance cameras cameras and likely captures images of you and other people? ?
- What do you think would be most important features to know about video surveillance? (prompts, policy? Technology?)
- Do you know what facial recognition software is? (if yes, what do you know about it?)
- Have you heard anything about video analytics? (If yes, what do you know about it?)

- Would you like to be able to tell where cameras are located and where you might be recorded?
- How would you like to be notified about camera locations?
- Would you use a smartphone app that lets you see where video surveillance cameras are located or lets you tag a camera location to let other people know it is there?

Group nine (legitimacy of purposes)

- Did you know that this organization (where we are standing) operates surveillance cameras and likely captures images of you and other people?
- What do you think of each of the following possible purpose for operating such camera surveillance:
  - to dispatch help if you needed assistance
  - to spot shoplifters or other crooks in the act and apprehend them
  - to locate people who have gone missing
  - to deter people from wrong-doing
  - to prosecute wrong-doers after some incident
  - to determine what type of person you are (eg your age, gender, race, or even your name) to better target advertising at you
- to determine what type of person you are (eg your age, gender, race, or even your name) to better apprehend or exclude those that the organization considers risky?

At the conclusion:

- **Demographic questions:**

- How old are you?
- What is your gender (observe)?
- What is your nationality?
- And, you live in Canada now? (ask/confirm if nationality is not Canadian)
- What is your highest level of education?
- What is your occupation or principal activities?

In depth follow-up interviews

- This would consist of covering some of the questions not addressed in the snapshot interview as described above, plus these additional questions:

- Have you ever had an experience where you were happy or relieved to know that there was a camera recording what was happening to you?
- Have you ever had an experience where you felt uncomfortable knowing there were surveillance cameras recording your actions?

- Would you like us to inform you of the results of our research?

Interview Guide: Rounds One and Two

"On the street" site of surveillance snapshot interviews
Due to the anticipated brief nature of these "man/woman on the street" interviews we plan to ask only 3-6 of these questions per participant and rotate the questions as we proceed with the interview process.

Group one (general awareness)

- Did you know that this organization (where we are standing) operates surveillance cameras and likely captures images of you and other people? Alternative: Did you know that you are being surveilled by video cameras when you are in this (public) space?
- Why do you think this organization conducts video surveillance?
- Did you spot any signs or notices that video surveillance is taking place?
- What do you think the organization does with the visual images of you and others that it captures? What do you think they should do, or not do, with them?
- How do you feel knowing that you may be viewed by the camera operators or others with access? Are you comfortable or uncomfortable knowing that?
- Does having video surveillance in this area help you feel more or less safe?
-

Group two (legal uses)

- Did you know that this organization (where we are standing) operates surveillance cameras?
- How do you feel about being recorded? Are you comfortable with it or does it bother you?
- Do you think of visual images--pictures or recordings of yourself—as personal information?
- Businesses that use video surveillance cameras sometimes give their recordings to police or other law enforcement agencies. How do you feel about that?
    - (if participant expresses concerns) what specifically are you concerned about?
    - (if participant says they're ok) Why do you feel comfortable with it?

- Do you think the police should have a warrant approved by a judge before getting access to video surveillance that they don't operate themselves?
- To what degree would it concern you if police had access to video surveillance without a warrant approved by a judge? (Provide a range: Not at all; a little, definite concern; a major concern.)

Group three (privacy rights, knowledge)

- The organisation we're standing in front of uses video camera surveillance. Do you think that this video surveillance should be covered by Canadian privacy law and regulation?
- Do you know whether or not the surveillance operator is supposed to inform you about this video surveillance?

I'm going to read a list of things you might or might not want to know about the way this organisation conducts video surveillance; for each one, I'd like to know if you think it is something you absolutely want to know about, would like to know about, or don't want/need to know about:

- who owns or operates the camera surveillance
- the purposes for which they are operating the camera surveillance
- how to contact the owner or operator
- whether someone is watching live
- whether help would come if you needed assistance
- whether your image was being recorded
- how long your images were kept before being deleted
- who had access to your images and for what purposes
- whether the video surveillance system was automatically analyzing your image to determine what type of person you are (eg your age, gender, race, or even your name
- ----------
- whether privacy complaints had been filed against the organization
- whether the organization had been found in violation of its privacy obligations, by the courts or the Privacy Commissioner

(Interviewer pick one of the items the participant answered "absolutely want to know" and ask why they feel strongly about that item) Why did you say that you absolutely want to know about X?

Group four (perceptions of surveillance)

- Did you know that this organization (where we are standing) operates surveillance cameras?
- Do you ever think about whether or not you're on camera when you walk around the city/mall?
- Do you behave differently if you know you're on camera?
- Do you think video surveillance benefits you as a [shopper/citizen/member of the public]? (if yes, how? If no, why not?)
- Did/do you avoid or resist the video surveillance system in any way? How?
- Would you like to see more, less or about the same amount of video surveillance? Why?
- Does having video surveillance in this area help you feel more or less safe?

Group five (knowledge about infrastructure)

- Did you know that this organization (where we are standing) operates surveillance cameras and likely captures images of you and other people?
- What do you think would be most important features to know about video surveillance? (prompts, policy? Technology?)
- Do you know what facial recognition software is? (if yes, what do you know about it?)
- Have you heard anything about video analytics? (If yes, what do you know about it?)
- Would you like to be able to tell where cameras are located and where you might be recorded?
- How would you like to be notified about camera locations?
- Would you use a smartphone app that lets you see where video surveillance cameras are located or lets you tag a camera location to let other people know it is there?
-

Group six (legitimacy of purposes)

- Did you know that this organization (where we are standing) operates surveillance cameras and likely captures images of you and other people?
- What do you think of each of the following possible purpose for operating such camera surveillance:
    - to dispatch help if you needed assistance
    - to spot shoplifters or other crooks in the act and apprehend them
    - to locate people who have gone missing
    - to deter people from wrong-doing
    - to prosecute wrong-doers after some incident
    - to determine what type of person you are (eg your age, gender, race, or even your name) to better target advertising at you
    - to determine what type of person you are (eg your age, gender, race, or even your name) to better apprehend or exclude those that the organization considers risky

At the conclusion:
Demographic questions:

- How old are you?
- What is your gender (observe)?
- What is your nationality?
- And, you live in Canada now? (ask/confirm if nationality is not Canadian)
- What is your highest level of education?
- What is your occupation or principal activities?
-

In depth follow-up interviews
This would consist of covering some of the questions not addressed in the snapshot interview as described above, plus these additional questions:

- Have you ever had an experience where you were happy or relieved to know that there was a camera recording what was happening to you?

- Have you ever had an experience where you felt uncomfortable knowing there were surveillance cameras recording your actions?

- Would you like us to inform you of the results of our research?

Interview Guide: Round 3

"On the street" site of surveillance snapshot interviews

- Why do you think this organization conducts video surveillance?
- Do you think of visual images--pictures or recordings of yourself—as personal information?

- Do you know whether or not the surveillance operator is supposed to inform you about this video surveillance?

I'm going to read a list of things you might or might not want to know about the way this organisation conducts video surveillance; for each one, I'd like to know if you think it is something you absolutely want to know about, would like to know about, or don't want/need to know about:

  - who owns or operates the camera surveillance
  - the purposes for which they are operating the camera surveillance
  - how to contact the owner or operator
  - whether someone is watching live
  - whether help would come if you needed assistance
  - whether your image was being recorded
  - how long your images were kept before being deleted
  - who had access to your images and for what purposes
  - whether the video surveillance system was automatically analyzing your image to determine what type of person you are (eg your age, gender, race, or even your name
  - whether privacy complaints had been filed against the organization
  - whether the organization had been found in violation of its privacy obligations, by the courts or the Privacy Commissioner

(Interviewer pick one of the items the participant answered "absolutely want to know" and ask why they feel strongly about that item) Why did you say that you absolutely want to know about X?

- Do you behave differently if you know you're on camera?
- Do you think video surveillance benefits you as a [shopper/citizen/member of the public]? (if yes, how? If no, why not?)Have you heard anything about video analytics? (If yes, what do you know about it?)
- Would you like to be able to tell where cameras are located and where you might be recorded?
- What do you think of each of the following possible purpose for operating such camera surveillance:
  - to determine what type of person you are (eg your age, gender, race, or even your name) to better target advertising at you
- to determine what type of person you are (eg your age, gender, race, or even your name) to better apprehend or exclude those that the organization considers risky

-

At the conclusion:

Demographic questions:

- How old are you?
- What is your gender (observe)?
- What is your nationality?
- And, you live in Canada now? (ask/confirm if nationality is not Canadian)
- What is your highest level of education?
- What is your occupation or principal activities?

Appendix B: Workshop Guide

(start and finish times may vary, length, 3 hrs)

9.00 – 9.10 Introduction
9.10 – 9.20 Warm up exercise (where do you stand?)
9.20 –10.00 Participant perceptions and categorizing
Begin Q & A/ discussion
10.00-10.20 Coffee break
10.20-11.20 Complete Q & A/discussion
11.20–12.00 Signage or app demo (if time permits)
Wrap up

Introduction

- introduction to the research and researchers
- voluntary participation and consent info
- goals and ground rules
- share the schedule for the workshop

Warm up

An exercise to orient the participants to some questions about the research in a fun and concrete way
Imagine there is a big line down the middle of the room. One end is the negative end, one the positive, and the middle is the neutral zone; think of it as a continuum. I'm going to call out some statements and I want you to position yourself along the line depending on how you feel. If the statement is the dumbest thing you ever heard and you completely disagree, go to the far end of the line in the negative zone. If it's transparently true and you couldn't agree more, go the positive end. And if you're somewhere between those two positions, find a spot that reflects your opinion along the continuum.

We're going to talk about these topics in various ways later, this is just to literally get a sense of where we stand as we begin the conversation.

Sample Statements:
· If I'm in a place where I know there is video surveillance, I feel safer.
· If I'm being watched or recorded I should be notified that it's happening.
· Cameras in airports should be used to help figure out who looks suspicious.
· Cameras in stores should be used to help figure out who should get special offers based on their shopping behaviour.

Now take a look up and down the line, and when you go to sit down, try to make sure you're beside someone you see standing in a different spot than you.

To begin

Everyone has a stack of Post-It® notes. Write down 3 things that come to mind when you think of video surveillance or CCTV. It might be one word that comes to mind, or a sentence. It has to fit on the paper so keep it simple. While you're doing that, I'm going to stick up some category titles that we've generated from earlier research. When you are done, come stick your notes up here on the wall under the category you think is most appropriate. If it doesn't fit in any of these categories, make your own category.

Categorizing

Titles: general awareness; legal uses; privacy rights/knowledge; perceptions of surveillance; infrastructure; legitimacy of purpose(s); information needs.

Discussion

Category by category, read out responses provided by participants and discuss. Depending on the direction of discussions, seed questions for each category may include:

General awareness

- Why do you think organizations conduct video surveillance
- Have you ever noticed any signs or notices that video surveillance is taking place? Where did you see them?
- What do you think organizations do with the visual images of you and others that it captures? What do you think they should do, or not do, with them?
- How do you feel knowing that you may be viewed by the camera operators or others with access? Are you comfortable or uncomfortable knowing that?
- Does having video surveillance in an area help you feel more or less safe?

Legal uses

- Do you think of visual images--pictures or recordings of yourself—as personal information?
- Businesses that use video surveillance cameras sometimes give their recordings to police or other law enforcement agencies. How do you feel about that?
    - if participant expresses concerns) what specifically are you concerned about?
    - (if participant says they're ok) Why do you feel comfortable with it?
- Do you think the police should have a warrant approved by a judge before getting access to video surveillance that they don't operate themselves?
- To what degree would it concern you if police had access to video surveillance without a warrant approved by a judge? (Provide a range: Not at all; a little, definite concern; a major concern.)

Privacy rights, knowledge

- Do you think that video surveillance activities should be covered by Canadian privacy law and regulation?
- Do you know whether or not a surveillance operator is supposed to inform you about this video surveillance?
- I'm going to read a list of things you might or might not want to know about the way this organisation conducts video surveillance; for each one, I'd like to know if you think it is something you absolutely want to know about, would like to know about, or don't want/need to know about:
    1. who owns or operates the camera surveillance
    2. the purposes for which they are operating the camera surveillance
    3. how to contact the owner or operator
    4. whether someone is watching live
    5. whether help would come if you needed assistance
    6. whether your image was being recorded
    7. how long your images were kept before being deleted
    8. who had access to your images and for what purposes
    9. whether the video surveillance system was automatically analyzing your image to determine what type of person you are (eg your age, gender, race, or even your name
    10. whether privacy complaints had been filed against the organization
    11. whether the organization had been found in violation of its privacy obligations, by the courts or the Privacy Commissioner

Perceptions of surveillance

- Do you ever think about whether or not you're on camera when you walk around the city, into a store or through a mall?
- Do you behave differently if you know you're on camera?
- Do you think video surveillance benefits you as a [shopper/citizen/member of the public]? (if yes, how? If no, why not?)
- Did/do you avoid or resist the video surveillance system in any way? How?
- Would you like to see more, less or about the same amount of video surveillance? Why?
- Does having video surveillance in this area help you feel more or less safe?

.

Knowledge about infrastructure

- What do you think would be most important features to know about video surveillance? (prompts, policy? Technology?)
- Do you know what facial recognition software is? (if yes, what do you know about it?)
- Have you heard anything about video analytics? (If yes, what do you know about it?)

- Would you like to be able to tell where cameras are located and where you might be recorded?
- How would you like to be notified about camera locations?
- Would you use a smartphone app that lets you see where video surveillance cameras are located or lets you tag a camera location to let other people know it is there?

Legitimacy of purposes

What do you think of each of the following possible purpose for operating such camera surveillance:

to dispatch help if you needed assistance
to spot shoplifters or other crooks in the act and apprehend them
to locate people who have gone missin
to deter people from wrong-doing
to prosecute wrong-doers after some incident
to determine what type of person you are (eg your age, gender, race, or even your name) to better target advertising at you
to determine what type of person you are (eg your age, gender, race, or even your name) to better apprehend or exclude those that the organization considers risky

Information needs

- Do you think organisations should have to tell you more about why they use video surveillance and what they do with the information they collect about you?
- How could they do that in a way that would be helpful or interesting to you?
- Where would you go or what would you do if you were interested in finding out information about video surveillance or your privacy rights?
- Who should be responsible for communicating or making sure that general · information about video surveillance and privacy is accessible to you if you want to learn about it?
- How important do you think it is to make sure organisations are obeying privacy law when they conduct video surveillance? 1-5 scale, with one being very important and 5 not important at all.
-

If time permits/alternate activities:

Signage

Show an example of a sample CCTV notification sign. What do you think, does it have enough information?

Thinking about the information needs we talked about earlier, what else would you like to see on this sign?

Show an example of a model sign that has all of the information to meet the Office of the Privacy Commissioner's recommendations for notification of overt video surveillance.

What do you think? Would you read all of this? Is it understandable? Is it necessary?

Smartphone Application

Demonstrate smartphone camera tagging application and discuss.

Wrap up

- Summary
- Thanks
- Options for further participation

Appendix C: Selected Literature

Visual Surveillance References with abstracts

CCTV

Beaumont, Ela. (2005). “Using CCTV to study visitors in The New Art Gallery, Walsall, UK.” Surveillance & Society 3 (2/3): 251-269.

Abstract
The routine use of CCTV surveillance in new art galleries in the UK presents an opportunity for researchers to harness its potential as a powerful observational tool in visitor studies, and recent developments in video technology have created new possibilities for observational research. Recent studies using video observation methods in the UK, France and the US have demonstrated how powerful film data can be, but have also shown the difficulties in operationalising studies that use these techniques. The analysis of video data is in its infancy in the field of art gallery visitor studies, and this paper contributes to the theoretical, ethical and practical debate by discussing a recent observational visitor study using in-house CCTV cameras in the New Art Gallery, Walsall. The study demonstrates significant advances on previous observational visitor studies that have gathered 'covert observational data'. It show how CCTV footage can be used to gather naturally occurring visitor activities in a highly structured way, without disrupting the gallery with extra cameras or microphones and yielding increasingly detailed, useful information. It opens up the prospect of a wider ideological debate about the use of CCTV in art galleries, and contributes to work in progress on a code of ethics for video observation in visitor studies.

Cameron, Heather. (2004). “CCTV and (In)dividuation.” *Surveillance & Society* 2(2/3): 136-144.

Abstract
This essay draws on work of Freud and Foucault to understand emerging converging aspects of visual surveillance and tracking technology. It discusses some of the general problems with video surveillance – due to its reliance on a flattened version of the visual realm, its partial view, and assumptions about human vision. It then moves on to show how CCTV has changed from the monitoring of flows to identifying individuals and functioning as the human interface for new databank applications, using Foucault's reflections on governmentality. The essay ends by detailing a controversial test of video surveillance and RFID tags which point out some new dangers for us to consider, and argues that we should resist the 'flat fantasy' offered by video surveillance.

Carroll-Mayer, Moira, Ben Fairweather& Bernd Carsten Stahl. (2008). “CCTV identity management and implications for criminal justice: some considerations.” *Surveillance & Society* 5(1): 33-50.

Abstract
The UK Presidency of the European Union called for an expansive, mandatory policy of surveillance technologies aimed at the reduction of crime and the protection of citizens. Research indicates that the efficacy for this task of the technology, epitomised by CCTV, cannot be taken for granted. This paper asks whether the effects of the technological surveillance environment may be more problematic than currently posited in the literature to the extent that they render more vulnerable and undermine the identities of those they are pledged to safeguard. Much of the literature in surveillance studies debates whether surveillance technology, particularly CCTV, has the effects of crime reduction and prevention attributed to it by proponents. This paper goes one step further and through a process of critical analysis explores the import for individuals subjected to the process of surveillance technologies epitomized by CCTV. In particular the paper addresses the question as it is perceived through the postmodernist agenda. Accordingly in the process of critical analysis the paper considers the effects of transcarceration, the phenetic fix and the technological imperative.

Cole, Mark. (2004). “Signage and surveillance: Interrogating the textual context of CCTV in the UK.” *Surveillance & Society* 2(2/3): 430-445.

Abstract
The UK is one of the most surveilled societies in the World. CCTV systems prevail in both private and public space. Since 2000, a Code of Practice has required that signage is clearly deployed to advise of the existence of those systems wherever they are in use. Throughout 2002, examples of that signage were captured photographically, culminating in an exhibition of this material in October of that year. While arguing that the signage works closely in conjunction with the technological systems to which it refers, this paper focuses on this textual superstructure, using a Foucauldian approach as a means of shaping the discussion. It concludes that the signage itself has a number of possible effects. Most significantly, it argues that these texts, outwith the technological structures to which they refer, actively and substantially facilitate the 'automatic functioning of power'.

Coleman, Roy. (2004). “Reclaiming the streets: Closed circuit television, neoliberalism and the mystification of social divisions in Liverpool, UK.” *Surveillance & Society* 2(2/3): 293-309.

Abstract
The normalisation of camera surveillance on the streets of the UK raises profound questions about the strategies of contemporary urban political rule and the material and ideological re-mapping of urban space. Firstly, this paper will argue that an understanding of street camera surveillance requires a consideration of the operation of neoliberalism at the local level [in this case Liverpool on the north west coast of England] through a myriad of 'partnership' arrangements that have shifted the terrain of local democracy and the

meanings of both the public interest and social justice. Secondly, in using case material from a paradigmatic neoliberalising city, the paper argues that surveillance cameras are part of a social control strategy that seeks to hide the consequences of neoliberalisation in creating a particular ambience and exclusivity regarding 'public' spaces. Thirdly, the paper critically considers whether we can understand visual surveillance as a technique for the 'exclusion of difference' in urban space or as a tool that suppresses the reality of social divisions.

Dubbeld, Lynsey. (2004) “Protecting Personal Data in Camera Surveillance Practices.” Surveillance & Society 2(4): 546-563.

Abstract
This paper explores in which ways privacy (in particular, data protection principles) comes to the fore in the day-to-day operation of a public video surveillance system. Starting from current European legal perspectives on data protection, and building on an empirical case study, the meanings and management of privacy in the practice of Closed-Circuit Television (CCTV) will be discussed in order to identify the ways in which data protection is addressed in the operation of a video surveillance system. The case study suggests that views expressed by actors involved in the use of CCTV and the organisational and technical measures that have been employed, are related to a number of data protection issues, in particular principles regarding data quality. In addition, the case shows that while regulations (consisting in particular of organisational procedures) pertaining to the permissibility of data processing can be discerned in the practice of centralised CCTV, few indications exist that mechanisms taking into account data subjects' rights were established. Therefore, the system of video surveillance discussed in this paper suggests that different elements of data protection feature in different ways in the context of CCTV. This finding gives clues as to future research on privacy and camera surveillance.

Fussey, Pete. (2007). “An interrupted transmission? Processes of CCTV implementation and the impact of human agency.” *Surveillance & Society* 4(3): 229-256.http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3449/3412

Abstract
This paper examines the processes that bring about the creation of new public-space CCTV schemes. Through an appraisal of the grounded activities of the practitioners who make decisions over CCTV, the role of agency is identified as a particularly strong, yet relatively neglected, influence on its implementation. Moreover, beyond dichotomised notions of central structures and local agency, an understanding is developed of the complex interaction between the individual actors involved in CCTV dissemination and the political context in which they operate. In doing so, public policy is identified as the vehicle through which camera surveillance systems become installed and disseminated throughout public space. Moreover, these various forces of structure and agency become filtered through identifiable networks of policy-makers, comprising 'responsibilised' actors who oversee the deployment of CCTV. This analysis is used to revisit a range of administrative and

theoretical understandings of surveillance, including: citations of CCTV as an evaluated response to crime; the attribution of power- and interest-based agendas to its implementation; and accounts which locate CCTV expansion within various evolving societal processes. Drawing on qualitative fieldwork data gathered during doctoral research, the paper considers the activities of practitioners at a local level and identifies crucial contexts, drivers and negotiations on which expanding surveillance is contingent. Ultimately, it is argued that the process of CCTV installation – from conception to material implementation – is disrupted and mediated by a range of micro-level operations, obligations, processes, managerial concerns (particularly conflict resolution and resource issues), structures and agency, and the indirect influence of central government. These not only arbitrate over whether the CCTV becomes installed, but also generate a range of additional uses for the cameras, many of which are performed before they are even switched on. This emphasises the need to consider the processes that enable and constrain the actions of those making decisions over CCTV and demonstrates how no single interest becomes solely participant in the deployment of surveillance. Finally, because of the centrality and contingency of both human agency and the structural contexts in which it operates in determining the installation of CCTV, questions arise concerning the importance of integrative sociological theories in understanding the deployment of surveillance.

Fussey, Pete. (2004). “New Labour and new surveillance: Theoretical and political ramifications of CCTV implementation in the UK.” *Surveillance & Society* 2(2/3): 251-269.

Abstract
This paper examines the implications of New Labour's approaches to crime and disorder on CCTV implementation. It concentrates on the usage of CCTV as one of the government's many initiatives, which are intended to address crime and disorder, including the fear of crime. In particular, the impact of the 1998 Crime and Disorder Act (CDA) - the cornerstone of this government's approach to crime reduction - on the generation of such strategies is examined. The paper revisits neo-Marxist and Foucauldian analyses of the so-called surveillance society through an appraisal of the complex relationship between structure and agency in the formulation and implementation of anti-crime and disorder strategies. Drawing on fieldwork data the paper considers the activities of practitioners at a local level by focusing on the influence of central government, local communities and 'common sense' thinking based on certain criminological theories. It is argued that a myriad of micro-level operations, obligations, processes, managerial concerns (particularly conflict resolution and resource issues), structures and agency - as well as the indirect influence of central government - shape CCTV policy. Ultimately, the creation of new local policy contexts under the CDA emphasise the need to consider incremental and malleable processes concerning the formulation of CCTV policy. In turn, this allows a re-examination of theoretical accounts of surveillance, and their attendant assumptions of sovereign or disciplinary power.

Gallagher, Caoilfhionn. (2004). “CCTV and human rights: the fish and the bicycle? An examination of Peck v. United Kingdom (2003) 36 E.H.R.R. 41. *Surveillance & Society* 2(2/3): 270-292.

Abstract
This paper analyses and considers the impact of a landmark decision by the European Court of Human Rights in January 2003 which highlighted the inadequacy of U.K. law in protecting the privacy of individuals captured on closed-circuit television (CCTV) cameras in public places. The domestic and Strasbourg decisions in the Peck case are assessed. Analysis of the subsequent responses of Government, the Courts and the media demonstrates that the lessons of Peck have yet to be learnt, and the Human Rights Act 1998 has failed to 'bring rights home' when it comes to Article 8 of the European Convention on Human Rights (ECHR), which guarantees the citizen the right to respect for private life. Privacy in the U.K. is now at best a residual right: what's left after each of an array of competing concerns have their say.

Gras, Marianne L. (2004). “The legal regulation of CCTV in Europe.” *Surveillance & Society* 2(2/3): 216-229.

Abstract
This paper explores the recent history of CCTV system regulation in England and Wales questioning whether recent additions to the law can be regarded as providing for effective regulation, in particular, of camera numbers. It goes on to explore the legal landscape relating to public and private use of CCTV to subject publicly accessible space to surveillance in Germany as well as giving an overview of the regulatory systems in France, the Netherlands and Sweden. Drawing from this analysis, minimum standards for effective regulation are explored in terms of fulfilling both the letter and the spirit of laws across Europe.

Groombridge, Nic. (2008). “Stars of CCTV? How the Home Office wasted millions—a radical ‘Treasury/Audit Commission’ view.” *Surveillance & Society* 5(1): 73-80.

Abstract
This paper looks back on earlier pieces on CCTV in Britain by Groombridge and Murji and argues that the identified failures of CCTV, in terms of effectiveness and value-for money, have been consistently ignored both at the time and in more recent government evaluations.

Helton, Frank & Bernd Fischer. (2004). “Reactive attention: Video surveillance in Berlin shopping malls.” *Surveillance & Society* 2(2/3): 323-345.

Abstract
The paper examines the practice of use of video-surveillance in Berlin Shopping Malls. The video systems observed here do not seem to be an efficient instrument of social control and exclusion. They are used more on demand for various purposes such as the monitoring of daily tasks and the co-ordination of persons working inside the mall. The objectives publicly claimed by management – crime prevention and the like – could not be achieved because the everyday practice presents other tasks to the operators. The workplace, the personnel,

their multiple tasks, their qualifications support more a reactive use of video surveillance than a proactive targeted observation of individuals, even if the equipment would allow for that. It may turn out that the CCTV infrastructure of Berlin shopping malls can be characterised best as test-beds – open for various applications. There are, however, obstacles to this in the form of data protection concerns and the lack of political and economic support to go further (tied of course to financial constraints). Finally, as shown in our study, the social practice in everyday life continues to resist one-dimensional expectations of the technological possibilities of CCTV.

Hempel, Leon. (2006). “In the eye of the beholder? Representations of video surveillance in German public television.” *Surveillance & Society* 4(1/2): 85-100.

Abstract
This article is based upon an analysis of the commonalities between CCTV and television. Although this article is not meant to contribute to media studies as a science, it will nonetheless use empirical data from diverse TV shows, time periods and regions to show the decisive role television plays in public acceptance and implementation of public surveillance technology, as well as in the construction of suspicion. Additionally, this article considers the technological similarities of CCTV and television by using TV data as a source of ethnographic material to understand the discriminating nature of visual surveillance technologies.

Klauser, Francisco. (2004). “A comparison of the impact of protective and preservative video surveillance on urban territoriality: The case of Switzerland.” *Surveillance & Society* 2(2/3): 145-160.

Abstract
This paper focuses on a comparison between two forms of video-surveillance and their consequences for the territoriality of public space users: the preservative, which aims to preserve public order and to prevent 'anti-social' behaviour; and the protective, which protect specific risk-points like buildings or objects. The fundamental difference between preservative and protective surveillance is linked to the spatial logic of its functioning, that can be deduced both from the position of the cameras and the general orientation of its view. Following Lefebvre and Raffestin, it argues that these socio-spatial relationships of social players may be considered as an inherent part of public space. In consequence, their transformation directly affects the qualities of public space. These theoretical explored are illustrated with a cartographical study of the cameras within the city centre of Geneva and a study of public sensitivity and perception of video surveillance in the Swiss city of Olten.

Lomell, Heidi Mork. (2004). “Targeting the unwanted: Video surveillance and categorical exclusion in Oslo, Norway.” *Surveillance & Society* 2(2/3): 346-360.

Abstract

The rise of video surveillance in the United Kingdom, in the form of the public installation of closed circuit television (CCTV), has been seen by several scholars as a contributing factor to the increasing exclusion of unwanted categories of people from city centers, a development often referred to as the 'commercialization' or 'purification' of the city. Drawing from field observations over three years in control rooms in Oslo, Norway, this article discusses whether CCTV systems in Oslo contribute to a similar process of exclusion. To do so, I compare the open street video surveillance system with two other CCTV systems - a shopping mall and a major transport center. The introduction of open street CCTV in Oslo in 1999 did not create social exclusion, but recent developments show the possibility remains. Although drug addicts and young people were the primary targets of surveillance in all three sites studied, ejections varied considerably from site to site. The shopping mall system had a higher ejection rate than the open street system, and was therefore the system with the clearest exclusionary effects. Reasons for the different ejection rates are discussed, in particular the social structure of the site under surveillance and the organizational relationships of CCTV operators to the policing agents connected to the surveillance system.

Macnish, Kevin (2012). “Unblinking eyes: the ethics of automating surveillance.” *Ethics and Information Technology* 14(2): 151-167.

Abstract
In this paper I critique the ethical implications of automating CCTV surveillance. I consider three modes of CCTV with respect to automation: manual (or non-automated), fully automated, and partially automated. In each of these I examine concerns posed by processing capacity, prejudice towards and profiling of surveilled subjects, and false positives and false negatives. While it might seem as if fully automated surveillance is an improvement over the manual alternative in these areas, I demonstrate that this is not necessarily the case. In preference to the extremes I argue in favour of partial automation in which the system integrates a human CCTV operator with some level of automation. To assess the degree to which such a system should be automated I draw on the further issues of privacy and distance. Here I argue that the privacy of the surveilled subject can benefit from automation, while the distance between the surveilled subject and the CCTV operator introduced by automation can have both positive and negative effects. I conclude that in at least the majority of cases more automation is preferable to less within a partially automated system where this does not impinge on efficacy.

Martinals, Emmanuel & Christophe Betin. (2004). “Social aspects of CCTV in France: The case of the city centre of Lyons.” *Surveillance & Society* 2(2/3): 361-375.

Abstract
Inaugurated a few days after the municipal elections in spring 2001 as a result of a campaign strongly formatted by security issues, the operation of CCTV in the centre of Lyons can be seen today as part and parcel of the security-oriented policies of the new socialist local government. Through responding in part to the concerns and interests of

those social groups which are more exposed to the problems posed by crime (particularly shopkeepers and residents), implementing such a policy contributes to the social construction of deviance. It not only acts to consolidate dominant social representations in the field of security, but the ways in which it is used lead to reformulation of the rules and social norms construing everyday practices and deviant behaviour in public space.

Minnaar, Anthony. (2007). "The implementation and impact of crime prevention / crime control open street Closed-Circuit Television surveillance in South African Central Business Districts." *Surveillance & Society* 4(3): 174-207.http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3447/3410

Abstract
The use and implementation of public open street Closed Circuit Television (CCTV) surveillance systems in Central Business Districts (CBDs) in South Africa solely for the purpose of crime control (reducing street crime) or crime prevention (deterrence) has in South Africa been a relatively new intervention within the broader context of crime prevention programmes. One of the drawbacks to its implementation for this purpose has been its costs and the inability of the South African Police Service to fund such implementation in the light of other more pressing priorities and demands on its finances and resources. However, the initiative to start implementing and linking CCTV surveillance systems in CBDs in the major metropolitan cities of South Africa to local police services was taken in the mid-1990s by Business Against Crime of South Africa (BACSA). This article, using case study overviews from four South African CBD areas (Cape Town, Johannesburg, Pretoria (Tshwane) and Durban), traces CCTV use as crime control or prevention surveillance, how they were implemented, the rationale behind their implementation and the operationalising of them in terms of preventing street crime and its uses in other surveillance. In addition it also looks at this initiative from the perspective of the growth and commercialisation of the management of these services, and the co-operation and co-ordination structures in partnership with the South African Police Service (SAPS). Furthermore, it reviews the purported impact on the reduction of crime of these systems in CBDs and finally the application of public crime surveillance by the CCTV control room operators (private security) in co-operation with the police (response team) and the role it plays in the observation, recording, arrest and conviction of suspects.

Muller, Christoph& Daniel Boos. (2004). "Zurich Main Railway Station: A typology of public CCTV systems." *Surveillance & Society* 2(2/3): 161-176.

Abstract
Railway stations have become places between 'public' and 'private'. In this exploratory case study, we are looking at the CCTV system at the Zurich main station, the largest railway station in Switzerland. This railway station is used by train passengers, by customers frequenting the station's shopping area, and by persons trespassing in the station. Looking at different types of CCTV systems, we examine the motivations that have been leading to the installation of the cameras, about their functionality and their effects on passengers and

customers. Based on our observations, we are going to present a typology of different uses of CCTV systems: (1) access control, (2) conduct control, (3) registering evidence, (4) flow control and the planning of deployment. As a conclusion, we will have a look at some future trends in the use of CCTV in railway stations, focussing on (a) individualization, (b) automation, and (c) commodification. In the last part of our presentation, we are going to ask about the limits of the spreading of CCTV systems in railway stations, focussing on the efficiency on one hand and on several possibilities for opposition on the other hand.hand.

Norris, Clive, Mike McCahill& Dave Wood. (2004). "The growth of CCTV: a global perspective on the international diffusion of video surveillance in publically accessible space." *Surveillance & Society* 2(2/3): 110-135. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3369/3332

Abstract
This editorial surveys the growth of video surveillance or Closed-Circuit Television (CCTV) throughout the world, setting the scene for this special double issue of Surveillance and Society, on the politics and practice of CCTV, and provides a brief introduction to the contents of the issue.

Ruegg, Jean, Valerie November & Francisco Klauser. (2004). "CCTV, risk management and regulation mechanisms in publicly-used places: a discussion based on Swiss examples." *Surveillance & Society* 2(2/3): 415-429.

Abstract
This paper focuses on the relations between different types of actors involved in both conceiving and using video-surveillance systems. More specifically, it deals with the reasons that support the growing use of video-surveillance systems, and the organisation structures and implementation schemes that are designed to cope with them. The analysis raises issues linked to the complexity of social and spatial relations that CCTV tends to produce. Based on four Swiss case studies chosen in function of different objectives (risks), different types of public spaces that are under surveillance (city centre, motorway, industrial zone, public transport), as well as different stages of completion of a CCTV project, the main results are to document new categories of actors: the definition of the relationship between CCTV-providers and end-users must be enlarged. Many more actors are playing important roles in terms of risk management and decision making while designing and implementing CCTV systems. Risks under surveillance: different types of risks are under surveillance. The study is underlining that different forms of surveillance must be distinguished, given the spatial characteristics of every risk (diffuse, located, specific and/or territorialized). The 'distancing effect': CCTV obviously creates distance between the object and the place where surveillance is actually made. To go a bit further, the paper claims that several kinds of distancing effects should be considered. These distancing effects modify both the quality of places under surveillance and the general context where mechanisms can be designed and implemented for a better public regulation of CCTV uses.

Saetnan, Ann Rudinow, Heidi MorkLormell&CarstenWiecek. (2004). “Controlling CCTV in Public Spaces: Is privacy the (only) issue? Reflections on Norwegian and Danish observations.” *Surveillance & Society* 2(2/3): 396-414.

Abstract
This paper examines data from an observation study of four CCTV control rooms in Norway and Denmark. The paper asks whether issues other than privacy might be at stake when public spaces are placed under video surveillance. Starting with a discussion of what values public spaces produce for society and for citizens and then examining CCTV practices in terms of those values, we find that video surveillance might have both positive and negative effects on key 'products' of public spaces. We are especially concerned with potential effects on social cohesion. If CCTV encourages broad participation and interaction in public spaces, for instance by increasing citizens' sense of safety, then CCTV may enhance social cohesion. But the discriminatory practices we observed may have the opposite effect by excluding whole categories of the populace from public spaces, thus ghettoizing those spaces and hampering social interactions. Though tentative due to limited data, our analysis indicates that structural properties of CCTV operations may affect the extent of discriminatory practices that occur. We suggest that these properties may therefore present 'handles' by which CCTV practices can be regulated to avoid negative effects on social cohesion.

Smith, Gavin J.D. (2007). “Exploring relations between watchers and watched in control(led) systems: Strategies and Tactics.” *Surveillance & Society* 4(4): 280-313.http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Criminal%20Justice%202

Abstract
Using ethnographic observation within a number of Closed Circuit Television (CCTV) control rooms as evidence, this paper documents the apparently trivial but subjectively meaningful types of technologically mediated interaction taking place between CCTV operators and those watched. It examines the operators' interpretations of the various incidents, individuals and social realities observed. In so doing, the author suggests a number of interesting social-phenomenological processes are occurring. These include: the formation and existence of disembodied relationships between watchers and watched across distanciated CCTV surveillance networks; an operator gaze incorporating care, control and creativity; the existence of hermeneutical narrative constructions among the operators. The latter practice can be empirically demonstrated through the operators' creation of 'celebrity characters', their attribution of pseudo-identities for cameo 'guest stars' and their playful characterisation of the framed action taking place in the spaces under observation. It is argued that such informal tactics, employed to both entertain and relieve pressure, are the unintended outcome of systemic strategies of control designed to induce conformity. They allow the operators to make sense of, bring meaning to and cope with relentless, often disjointed, imagery and with the emotional strain of the CCTV workplace culture. The paper also suggests

that tactics are not limited to the watchers. The watched or Stars of CCTV appear to employ methods in a similar bid to manoeuvre themselves around the cameras. By considering the practices of watchers and watched, it is argued more generally that CCTV technology is a social medium, the people, places and objects watched functioning not simply as passive 'objects of information', but also as active 'subjects of communication'.

Smith, Gavin. (2004). “Behind the screens: Examining constructions of deviance and informal practices among CCTV control room operators in the UK.” *Surveillance & Society* 2(2/3): 376-395.

Abstract
Hitherto, limited empirical research has focussed on the micro-level dynamics and social interactions forming a typical CCTV control room's everyday operational culture. As such, the 'human element' behind the monitoring of the cameras has been largely ignored in much CCTV analysis to date. Drawing upon ethnographic observation conducted within a privately funded CCTV control room, this paper questions the accuracy of a central assumption made in much of the general literature on CCTV, namely that surveillance cameras are not only controlled and monitored constantly, but also operated effectively and efficiently. A consideration of the types of person monitored, and why certain individuals attracted attention from the operatives, is also given. More specifically, and drawing on knowledge gleaned from studies of workplace culture, the article also identifies subtle forms of workplace resistance occurring in the observed control room's informal organisation. This involved strategies such as time wasting and game playing being adopted by the operators, largely in response to the effects of tiredness, boredom, derision and the difficulty of effectively monitoring up to fifteen television screens simultaneously. Indeed, the findings from the research suggested that the operatives felt alienated from their job, due to the imprisoning confines of the CCTV control room, the long hours worked, the high expectation levels placed upon them and the low pay and lack of acclamation received from their employers. Reflecting on these findings, it is concluded that, taken together, the above factors seriously undermine the effectiveness of CCTV surveillance per se.

Stedmon, Alex (2011). “The camera never lies, or does it? The dangers of taking CCTV surveillance at face value and the importance of human factors.” *Surveillance & Society* 8(4): 527-534.http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4192

Abstract
How many of us question what we’re shown via closed circuit television (CCTV) as being the truth of a situation? Can clear and easily identifiable images be wrong? And if they are, how can you argue against the power of the recorded image from a legal standpoint? Can Human Factors help us improve surveillance for society? In this real example of improper CCTV surveillance, can CCTV always be taken at face value? The simple answer is no, but how many people accept what they’re shown without question and end up paying the penalties? This paper examines a case study where all that appeared on the CCTV image was not as it seemed. It then considers the underlying human factors issues of CCTV

technologies for surveillance and the importance of understanding the fundamental human-machine interface.

Sutton, Adam & Dean Wilson. (2004). “Open-street CCTV in Australia: The politics of resistance and expansion.” *Surveillance & Society* 2(2/3): 310-322.

Abstract
This paper summarizes the first systematic attempt to document and assess the extent of open-street CCTV systems in Australia. In addition to providing empirical data, this paper argues that it is tempting for Australian scholars, and those elsewhere, to view the UK 'surveillance revolution' as the harbinger of inevitable global trends sweeping across jurisdictions. However analysis of the Australian data suggests that the deployment of CCTV in other national contexts may follow substantially divergent patterns. While the Australian CCTV experience follows many trends exhibited in other nations, it is nevertheless significant that the diffusion of CCTV in Australia has been more restrained than in the UK. We suggest that the divergence between the UK and Australian experiences resides in contrasting political structures and the consequent variation in the strength of debate and resistance at the local level.

Timan, Tjerk& Nelly Oudshoorn. (2012). “Mobile Cameras as New Technologies of Surveillance? How citizens experience the use of mobile cameras in public nightscapes.” *Surveillance & Society* 10(2): 167-181.

Abstract
In Surveillance Studies the terms ‘sousveillance’ and ‘inverse surveillance’ describe forms of surveillance that have a bottom-up and democratic character. However, in this paper this democratic notion is questioned by looking into practices and experiences with both Closed Circuit Television (CCTV) and mobile cameras by Dutch citizens. By interviewing in the nightlife district of the Rotterdam city centre, data has been gathered on both mobile- and CCTV camera confrontations. From this, an exploration is made into how mobile cameras are experienced in the nightlife landscape. Comparing these experiences with CCTV provides insight into new surveillance issues that emerge due to the mobile camera. The perspective of analyzing surveillance technologies as hybrid collectives that may take different shapes in different places, allows for a contribution that attempts to improve our understanding of the current changes in the surveillance technology landscape.

Wakefield, Alison (2004). “The public surveillance functions of private security.” Surveillance & Society 2(4): 529-545.

Abstract
This paper is concerned with arguably the most pervasive body of watchers in society, private security personnel. Set in the context of the rapid post-war expansion of both mass private property and private security, the contention of the paper is that the inter-

dependency between these two industries is key to understanding the significance of surveillance as a form of governance in privatised urban spaces. Drawing on an empirical study of private security in three settings: a cultural centre, a shopping centre and a retail and leisure complex, it is argued that surveillance practices represented much more than an approach to policing and crime prevention in these venues, and were central to broader management strategies for the three centres. These surveillance practices also became the basis for collaborative working with the police. In the conclusion, a number of concerns are raised with respect to the policing aspects of surveillance, in relation to both commercial and public policing objectives and the human rights and civil liberties being eroded along the way.

Walby, Kevin. (2006). “Little England? The rise of open-street Closed-Circuit Television surveillance in Canada.” Surveillance & Society 4(1/2): 29-51.

Abstract
Social monitoring is often explained in terms of top-down or hierarchal forms of power, which is reflected in the reliance on neo-Marxist and disciplinary society analytical frameworks in contemporary studies of open-street closed-circuit television (CCTV) surveillance. Established surveillance theories cannot account for instances when citizens themselves seek out regulatory measures in their own communities. Community schemes can precede and inform police policy. Drawing from developments in the sociology of governance, I examine media coverage, government document and questionnaire data regarding the rise of open-street CCTV schemes in Canadian cities, demonstrating empirically how regulation through CCTV surveillance can be generated from above (e.g. police, state), the middle (e.g. business entrepreneurs), and below (e.g. moral entrepreneurs and civic governance). Offering four suppositions that act as a pragmatic framework for understanding the rise of open-street CCTV in Canada, this article is a partial corrective to the reigning theoretical explanations regarding how regulatory projects like open-street CCTV are generated.

Webster, William R. “The diffusion, regulation and governance of closed-circuit television in the UK.” *Surveillance & Society* 2(2/3): 230-250.

Abstract
This article explores the introduction and diffusion of Closed Circuit Television (CCTV) surveillance systems in public places across the UK. In particular, it seeks to examine the diffusion of CCTV alongside the emergence of regulation and governance structures associated with its provision. By doing so, it is argued here, that the processes of diffusion, regulation and governance are inherently intertwined, that they have evolved together over time, and that we must place CCTV within its institutional and policy setting in order to have a good understanding of the reasons for its diffusion. Initially, it appears that the CCTV policy arena is relatively unregulated. This is surprising given the nature of the technology and its potential to be used as a tool for surveillance and control. However, a closer examination of its diffusion points to a variety of regulatory mechanisms emerging from within the CCTV policy environment and evolving alongside the development of policy networks. It is argued here, that whilst it may appear that regulation has emerged from

within these networks, government, despite limited legislative intervention, remains the dominant actor in the policy process through its ability to shape and influence networks.

Zurawski, Nils & Stefan Czerwinski. (2008). “Crime, maps and meaning: Views from a survey on safety and CCTV in Germany.” Surveillance & Society 5(1): 51-72.

Abstract
In researching CCTV, it must be examined how people assess CCTV measures against the background of their individual knowledge about the technology in question. Research on visual surveillance needs to ask how they sense and perceive cameras. As cameras impact on spatial images and social perceptions, such as security, people's confidence will not be explained solely by showing that cameras do or do not work in reducing crime. For that it is necessary to look at what expectations people have regarding CCTV and its possible shortcomings. These assumptions provided the research frame for a qualitative study that focused on the assessment of visual surveillance in an urban environment. The study examined what knowledge people actually had about the technology and what meaning was ascribed to the cameras themselves. It seems that knowledge does not inform the meaning, but that the ascribed meaning is generated independently of this knowledge or the lack thereof. The results permit the conclusion that forms of spatial perception that socially produce 'dangerous spaces' have gained prominence. Hazard is then directly ascribed to the spatial context itself. Thus, CCTV seems to be a suitable measure for safeguarding these 'crime hot spots' and is being used as a projection screen for fears and felt insecurities. Although an expansion of CCTV is mostly rejected in our study, CCTV measurement is seen as a suitable means to counter crime in particular spatial settings. The study indeed revealed many contradictions in the individual assessment of cameras in relation to actual knowledge and the meaning of these in relation to personal safety and spatial perception.
Note: potentially interesting bit on the ways people ascribe meaning to cameras based on perceptions/feelings of safety in particular places.

Facial Recognition

Introna, Lucas & David Wood. (2004). “Picturing Algorithmic Surveillance: The politics of facial recognition systems.” *Surveillance & Society* 2(2/3): 177-198.

Abstract
This paper opens up for scrutiny the politics of algorithmic surveillance through an examination of Facial Recognition Systems (FRSs) in video surveillance, showing that seemingly mundane design decisions may have important political consequences that ought to be subject to scrutiny. It first focuses on the politics of technology and algorithmic surveillance systems in particular: considering the broad politics of technology; the nature of

algorithmic surveillance and biometrics, claiming that software algorithms are a particularly important domain of techno-politics; and finally considering both the growth of algorithmic biometric surveillance and the potential problems with such systems. Secondly, it gives an account of FRS's, the algorithms upon which they are based, and the biases embedded therein. In the third part, the ways in which these biases may manifest itself in real world implementation of FRS's are outlined. Finally, some policy suggestions for the future development of FRS's are made; it is noted that the most common critiques of such systems are based on notions of privacy which seem increasingly at odds with the world of automated systems.