Report on:

Video Surveillance Regulation and Rights: Canadian's Information Needs

Prepared by
Joseph Ferenbok
Brenda McPhail
Alex Cybulski

Submitted to:

the Office of the Privacy Commissioner of Canada

as part of

the contributions funding research project #369529
Video Surveillance and Privacy: Who is Watching You? (and do you know why?)

July 15, 2013

Contents

Introduction: What Canadians do and do not know, and why it matters

This report is based on the findings of a broader research project called "Video Surveillance and Privacy: Who is Watching You? (and do you know why?)." The project took a snapshot of attitudes and knowledge of video surveillance practices and regulation in an urban centre in Canada. From the data gathered during focus groups and 'on-the-street' interviews we were able to see a number of trends. We observed that:

- respondents generally **did not know** about the regulation of video surveillance in public spaces (very few people interviewed were aware of PIPEDA);
- many **assumed** video surveillance was regulated or felt that if was not regulated that it should be;
- most participants **did not know** what was currently done with their personal information collected via video surveillance;
- and most of our participants **did not know** about video analytics or what could be done with their data using this technology.

This lack of knowledge does not suggest, however, that people are not interested in obtaining more information about the nature of video surveillance practice, policy and regulation. In fact, we learned that:

- the majority of our participants indicated that they **would like to know** the purpose(s) of surveillance
- participants also told us that they **would like to know** what was being done with their personal information by those collecting it, including how long it was being kept, who could access it, and what it might be used for.

These trends across our research suggest that Canadians would be receptive to a public discussion about video surveillance practices and policy. For this to be truly effective, however, given the lack of information that citizens currently possess about video surveillance, an educational campaign would be a critical first step in the discussion process.

Until citizens can understand that we are rapidly approaching a time when our faces and other biometrics can serve as gateways into our public and private identities, they are unlikely to understand the implications of video surveillance policy. Many participants, for example, 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 according to both PIPEDA and OPC guidelines. As our research has demonstrated, once these language and knowledge barriers were mitigated our participants were capable of engaging in meaningful dialogues regarding video surveillance, well beyond our scripted protocols.There is a clear role for the OPC, as part of the mandate to promote "public awareness and understanding of privacy issues" (OPC 2010), to provide the information Canadians need to understand the rapidly changing video surveillance landscape.

Background

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. However, these relatively recent and ongoing changes to video surveillance practices and technologies from digital sensors to cloud storage are generally hidden from surveillance subjects (Ferenbok & Clement 2012). Compounding the need for citizen education, a recent OPC funded research study (Clement et al. 2010) on private sector compliance with PIPEDA indicates widespread ignorance of the most basic requirements for video surveillance practices on the part of those collecting Canadian's video data. It seems clear that, in Canada, the private sector is either unaware of legislative requirements, or choose to interpret their responsibilities as narrowly as possible with respect to privacy guidelines for video surveillance.

This situation, where surveillance practices and technologies have outpaced policy and awareness, presents not only an opportunity for research, but also one for public outreach and education. A range of studies have been done internationally and in Canada around the deployment and efficacy of video surveillance, while in Canada, foundational research has begun

on video surveillance practices and policy (see: Dawson et al., 2009; Deisman et al., 2009). None of these studies, however, ask what Canadians know about video surveillance practices and policy nor do they address how best to inform Canadians about video surveillance issues in order to ensure an informed electorate.

One part of our Who's Watching You? project sought to determine what Canadians know and what they want to know about privacy policy and regulation around video surveillance practices in public spaces. Data was collected from people in brief interviews and a series of iterative focus groups/workshops with Canadian citizens in a major urban centre to provide a snapshot of the current state of knowledge and to gauge participant interest in acquiring further information about video surveillance practice, policy and regulation.

Context

While this study focused on conventional private sector camera surveillance, it is important to place Canadian's need for more information and education about their privacy rights in relation to visual surveillance in the context of rapidly changing technologies of visual surveillance. There are two advances in particular that will be significant for citizens and consumers. The first is video analytics, or video content analysis. These terms are used to describe computerized processing and analysis of video streams, particularly those captured by surveillance systems. These kinds of systems can perform real-time analysis of video, to detect events as they happen, or they may be used for retroactive analysis to extract data (Agent 2010). In the private sector, video analytics are increasingly being used to mine visual data to develop consumer profiles, enhance sales practices, offerings and techniques, and to target specific customers. While some of these practices may result in enhanced sales offerings that consumers may find beneficial, the fact remains that personal data is likely to be used without an individual's knowledge or consent, and this usage may have consequences for individuals ranging from preferential treatment to increased security monitoring. If people are unaware of these practices, or that this kind of activity is even a possible use of visual surveillance data, then there is little likelihood that organisations using this technology will feel obliged to be accountable or transparent in their practice.

The other technological advance that provides relevant context for the need for public education about video surveillance is 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. Technologies like Google Glass, that stream and archive video information, may mean that every conversation, event, and interaction--every stroll down the sidewalk--will produce traceable data that is both ubiquitous and surreptitious. 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 analyzed, it is likely that their perspective on what constitutes personal data will change. It will become increasingly important that people understand their own privacy rights, and the rights of others, as these technologies become more mainstream.

Methods

The Who's Watching You? Project worked to determine what Canadians know about visual surveillance practices and technologies using two complementary data collection methods, 156 person on the street interviews and a series of focus groups/workshop sessions to determine what people know about the video surveillance activities that are capturing their personal visual information . The methodologies employed are described in more detail in the primary research report resulting from this project, "Who is Watching You? And Why? What do Canadians know about their video/visual privacy?"

The three hour workshops were structured around 1) eliciting participant views, 2) getting participants to vocalize perceptions and categorize them based on headings developed from the on-the-street interview series, and 3) encouraging participants to envision or describe the kinds of systems they would like to see implemented. The workshops included an introductory exercise to determine where participants stood on issues of video surveillance and was then followed by group exercises which incorporated general questions to solicit participant's opinions and knowledge about video surveillance and included, in one iteration, a critical making exercise where volunteers built public spaces under surveillance. We used the interview questions and interview data obtained in a previous phase of the project and on the Office of the Privacy Commissioner of Canada's (OPC) March 2008 Guidelines for Overt Video Surveillance in the Private Sector, to reflect our focus on the surveilled rather than the surveillers. Part of the goal was 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 incorporated items such as examples of signage, either actual or models prototyped in previous research, or an android app designed to help people map surveillance camera locations as concrete artifacts that can encourage conversation about what information people want or need to know in order to exercise their privacy rights, and how they would like to be informed of those rights. We also encouraged people to imagine a design for a surveillance installation and describe it to the group. Data collection was done by note-taking and video recording. As part of the workshop process participants were asked to write down their key questions or insights on the current discussion question; these written documents do not include names or other identifying information and were collected and used as part of data analysis.

Recommendations

Our recommendations are based on a one year localized study that provides a snapshot of urban Canadian attitudes based on brief interviews, two in-depth focus group/workshops and a public forum. Based on the geographic limitations and sample size, it must be stressed that there are limitations in generalizability to the wider Canadian populace. However, the recommendations below also come as a result of many years work in the area of public video surveillance practices in Canada and are substantiated by the broader experience and networks of our research group.

Coalescing the discussion

Issues around the control of personal information and public video surveillance will reach a critical mass either reactively through a data breach or failure of systems to live up to expectations and promises, or proactively through education and debate. To take a proactive stance Canada needs
to mount a serious awareness and education campaign about visual privacy and video surveillance.
To promote a broader policy debate around privacy and video surveillance, there needs to be:

1. A public education campaign;

2. Standardized signage and information iconography;
3. Interactive and social engagement strategies

1. Public Education

In light of current and upcoming changes to frequency and depth of video surveillance practices a broad educational campaign is needed, focussing on video surveillance rights including the provisions of PIPEDA that support individual privacy and information rights specifically. Based on our interactions with our snapshot of Canadian citizens we believe it important to increase knowledge and awareness of:

- the existence of, and role of, the Privacy Commissioner of Canada and her office in protecting Canadian privacy rights including those related to video surveillance;
- PIPEDA (generally) and specific features of video surveillance regulation that are relevant to citizens;
- The status of video information as personal information;
- Rights of Canadians in public spaces (in relation to video surveillance); and
- The changing capabilities of video surveillance technologies (including: profiling or social sorting).

The campaign should be simple, direct and demonstrate personal value to individual citizens. Basic points that need to be included, based on information our participants told us they wished to know or be able to access, are:

- Video Surveillance is regulated in Canada;
- Video surveillance is governed by the Privacy Act and PIPEDA;
- Video data can be personally identifiable information;
- Citizens have the right to access personal information captured by video surveillance;
- Canadians have the right to know how their video information is used.

Based on our findings, we would suggest that a campaign should:

Focus on 'tangible' individual rights (with quick sound bites).
With the rise of social media people are increasingly aware of informational privacy online. Using the language and 'tangible' understandings of online information privacy to discuss video surveillance may be fruitful. For example, a tagline like "your image is your personal information" may link visual privacy online with surreptitious surveillance in public.

Tell personal stories (make narratives clear and personal)
Any information campaign must interpolate the citizen into the message. Often this was done with our participants when they shared personal stories about their experiences with public

surveillance practices. Linking law and regulations to personal narratives might be a good strategy for engagement.

Develop consistent imagery
This educational campaign should include the introduction of a standardized visual symbol for video surveillance (in Canada) which could then be used as a commonly recognised visual link to video surveillance information and signage.

2. Standardize Signage

Despite legal requirements, research has demonstrated that only just over a third of camera operators that survey publically accessible spaces deploy signage (Clement 2010). The Who's Watching You? project findings, as reported in the Final Report, also suggest that current signage practices are often ineffective. Undoubtedly the reasons for this are many and varied, ranging from a lack of knowledge on the part of organisations, to prioritizing of risk management and liability concerns or budget over full compliance in the area of surveillance signage. Whatever the underlying causes, surveillance signage may be omitted or 'down-played' by positioning small signs at entrances obscured from direct-line of sight or hiding surveillance notification signs in a sea of much bigger and brighter commerce-related signage.

Furthermore, when looking at the signs that do exist, there is a wide heterogeneity between them, and their informational value. Despite taking a critical attitude towards signage they had seen in the past, most of the participants in our focus groups felt signs were still an important way to communicate information to the public. This suggests that a codified system of signs with consistent iconography and information hierarchy could be used as both an engagement vehicle and as part of an information campaign. A common iconic language around video surveillance capabilities, purposes and information practices could help to coalesce discussion around issues of video surveillance. This kind of icon-based system to help Canadians to understand privacy and video surveillance practices and policy would require the OPC to take a leadership role in a broad scale personalized campaign that encourages Canadians to: "Know where YOUR information goes!" A uniform identity for signs and notices, etc, like the Genetically Modified Food labels in Europe, or food dietary contents labels, would be a significant step towards increasing awareness and bringing these issues into the public Canadian consciousness. As one participant suggested during our research, the OPC could potentially work with video

surveillance suppliers and vendors to include a sign template (or a printable electronic template for a sign) with every camera sold so that system operators have an easy mechanism to become compliant.

Some of the key visual elements for video surveillance signs based on the information needs identified by our respondents and focus groups, people want to be able to clearly understand at a glance:

- purpose of the surveillance
- scope of the surveillance
- live monitoring or emergency response services (safety)
- information retention and access
- contact information for citizens to obtain more information about surveillance policies

In general, our participants agreed on the principle that "the [surveying] organization" should provide people with information about the system so that they could "be held accountable." The ultimate test of signage should be its ability to assure citizens of the posting organisation's commitment to public accountability.

Most participants also agreed that a online mechanism for more information linked to physical signage would also be useful. The participants also groups also mentioned that they wanted to see the signage system based on a positive or empowering message (see Figure 2 in appendix 1), in addition to delivering useful information for citizens. This perhaps speaks to the need for a more citizen centric system of providing information about surveillance infrastructures.

3. Engage on Social Media

Given the penetration of ubiquitous computing devices and the popularity of new media to raise awareness of social issues it is important to consider how education about video surveillance might utilize these mediums to address critical knowledge gaps. During the street interviews respondents were divided as to whether they would use a smartphone application to help them locate public spaces under video surveillance or to know if it was taking place in their proximity. Many respondents thought such an application would be useful, but did not think it would be something they were interested in regularly using. Among those interviewed, many respondents also conceded that while the app might be useful, their phone did not have the technical capacity to run advanced applications, suggesting that smartphone penetration is not widespread enough

to cover all cellphone users. Although apps played a relatively small role in our discussions with participants during the "on-the-street" interviews, apps, and new media in general, took on a much more prominent role during the focus groups. While apps were discussed as one way to inform citizens about video surveillance, the internet topped even signage as the best channel to inform people about the presence and regulation of video surveillance.

At the second focus group meeting a prototype of the "SurveillanceWatch" smartphone app was demonstrated for those in attendance. While many participants felt it was an interesting idea, a few questioned the potential for mass adoption. Since our forum, an independent project on Kickstarter sought funding for an application with similar functions to the mobile software design by Professor Andrew Clement's SurveillanceWatch group (see Appendix 2). Unfortunately, as of the writing of this report, it doesn't look like this project, for an app called Surv, received enough funding to be successful. Despite this failure, the existence of this type of project on Kickstarter demonstrates that independent of the academy, pockets of tech savvy software designers and concerned individuals recognize the power asymmetries of current video surveillance practices and recognize the significance and potential of technology in helping to offset some of the imbalance.

New Media provides cost effective opportunities for public engagement and education at a much larger scale than ever before. The internet is stretching from a one-way information channel to a communication hub that facilitates networks and communities focused on complex social issues. Canada must turn to Social Media Channels to improve the effectiveness of how video surveillance policies and issues are disseminated. Social Media proved an excellent tool for recruiting participants and informing participants both about research events as well as content issues. This may be a significant mechanism for engaging a new generation of civically responsible citizens who are interested in issues of policy development around video surveillance. As a key component of its public education mandate, the OPC might consider hiring a policy / regulation Social Media Evangelist to maintain information streams around issues of privacy, technology and surveillance. Such a position would help improve the informational interaction between citizens on significant and complex social issues.

Outside of its role as a platform for educating Canadians, greater exposure to social media has given privacy issues greater exposure in public discourse. In many ways, controversies surrounding privacy on networks like Facebook, Linkedin and Myspace have created a discourse around information privacy that did not exist before these websites were popularly used. In addition, when interviewing Canadians about new surveillance technologies including video analytics, many of those interviewed related these developments to technologies they had already encountered, including facial recognition software running on Facebook which was capable of identifying them, or other users. This addresses an useful paradigm in

educating individuals about new technologies, by making comparisons to existing consumer technology. However, such comparisons have their limitations, as many new technologies do not have clear allegories in common consumer products.

Summary

We feel that a public education campaign associated with an online strategy and a standardized practice of signage/labeling will go a long way towards raising the awareness of Canadian Citizens to issues of video surveillance. Based on the findings of the Who's Watching You? project, most Canadians typically do not think much of video surveillance regulation or policy until the issue is raised; we found participants became more interested, and indicated in various ways that they were changing or developing ideas even during very brief interviews, as they became engaged with the questions we asked and thought through the issues. In the absence of active questioning, however, only when events bring video surveillance under scrutiny, as with the Boston 2013 bombings, do these issues catch public attention. And in the kinds of cases that receive intense media interest, video surveillance is often positioned as the solution to a problem, not as a tool with both advantages and disadvantages for citizens. The challenge for any awareness campaign around video surveillance is that people have become highly habituated to it, and are generally accepting of its utility without being fully informed of the uses to which the collected data may be put. In addition, many of the current and upcoming changes to video surveillance systems are hidden from average citizens. They happen on chips embedded in cameras and post capture video analysis by automated (a.k.a. smart) systems using signal processing. This process turns digital images and video into actionable information. The actions taken on this information, how the information is shared and with whom; where it is stored; and who has access to it all remain hidden from public view.

Video surveillance systems are becoming very different from the CCTV systems deployed in past. Demonstrating these changes and why they are important to privacy, democracy, freedom of speech and associating is a difficult challenge without concrete examples. Events like the Toronto G20 summit, the Vancouver riots and bombings in Boston earlier this year clearly demonstrate how large public tragedies are effective at jumpstarting debates over public video surveillance practices. Reactionary responses however are not necessarily the most effective means of building a participatory democratic society.

We observed that:

- Few people have any notion of 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 or who participated in our workshops/focus groups 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--they may not have known a great deal about the subject, but were interested enough to engage with researchers further. And the more they thought about the issues, the more questions they had, and the more suggestions they made. Certainly this seems to suggest that Canadians care enough about the specific purposes behind the uses of video surveillance that it would be helpful to initiate more public discussion and debate. This might also suggest that 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 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, bringing video surveillance not only to street level but also to every wired user, people's 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. Even in the absence of any concrete information, the citizens we spoke with displayed a remarkable faith that video surveillance in Canada could be, and should be, regulated to protect their individual rights and collective interests. One of our workshop participants expressed the stakes for Canadians as follows:

> Surveillance in general has the potential to limit our mobility. Video surveillance with new technologies have the ability to analyse us in undesirable ways that impinge on our privacy. Regulators need to analyse what is practical and regulate out problematic usage.

> Like our regulations limit police procedure, there should be laws limiting reasonable uses of surveillance. (Workshop participant, February 2013)

In other words, citizens expect that they will be protected by regulation and policy, and they need to know the extent to which this is the case. Significantly more work needs to be done in the area of raising public understandings of visual and video privacy. More in depth and broader research is needed around the most effective ways of educating the public and engaging with civil society to understand how Canadians want to shape their society with respect to video surveillance rights, and immediate efforts are required to educate Canadians about the challenges created by contemporary video surveillance, its legitimate use, and their rights.

References

Agent: Comprehensive Video Analytics Solutions. (2010). “What is Video Analytics?” Available: http://www.agentvi.com/20-technology-56-What_is_Video_Analytics

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

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.

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.

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

Appendix A: Select Focus Group Materials on Signage and Education

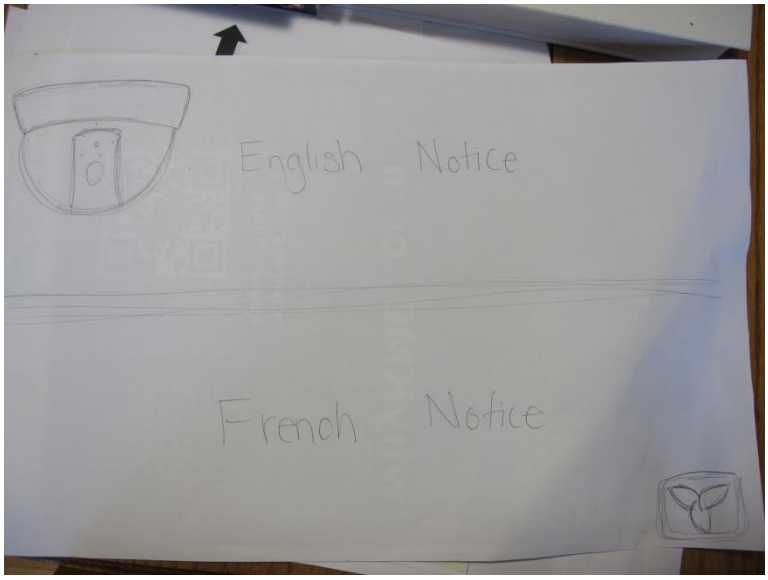

Figure 1: Bilingual Signage for sample

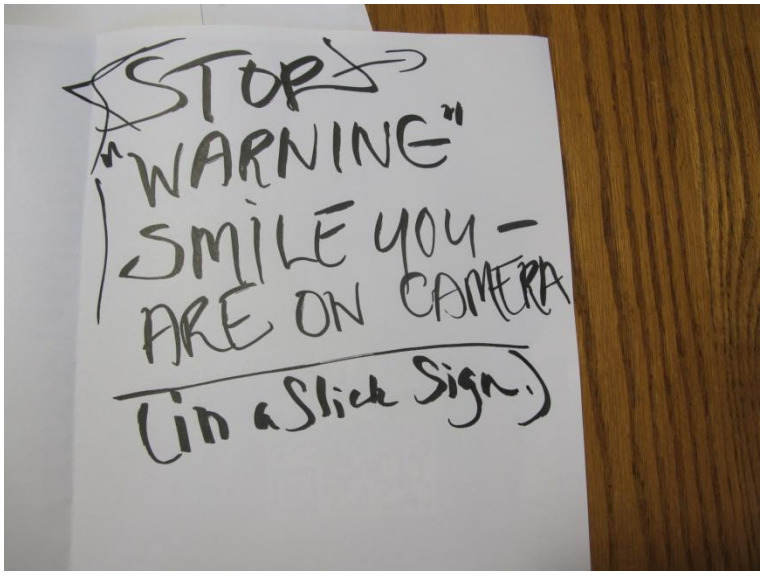

Figure 2: Education & communication sign idea

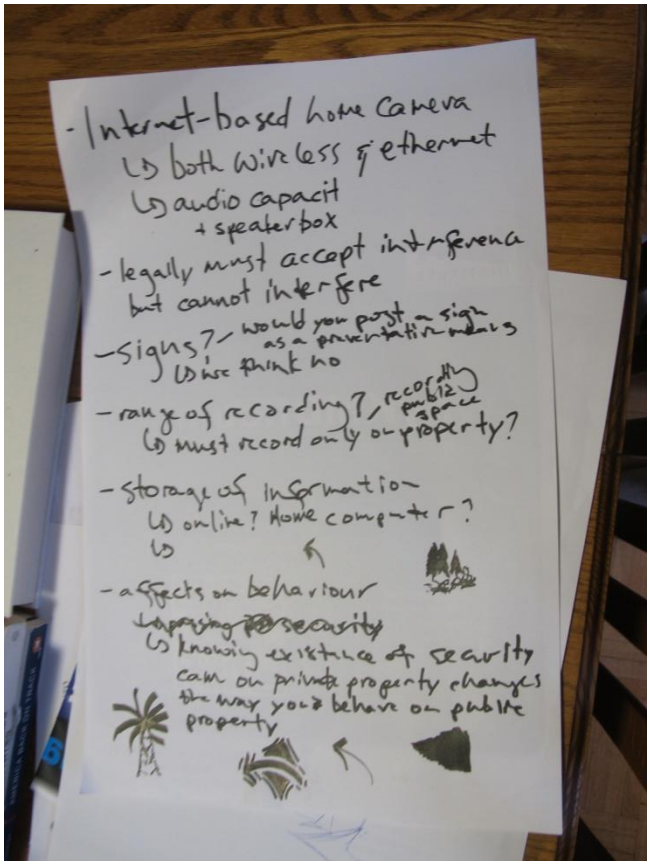

Figure 3: Notes on Private Surveillance issues

Appendix 2: Surv App

Figure 1: Kickstarter campaign

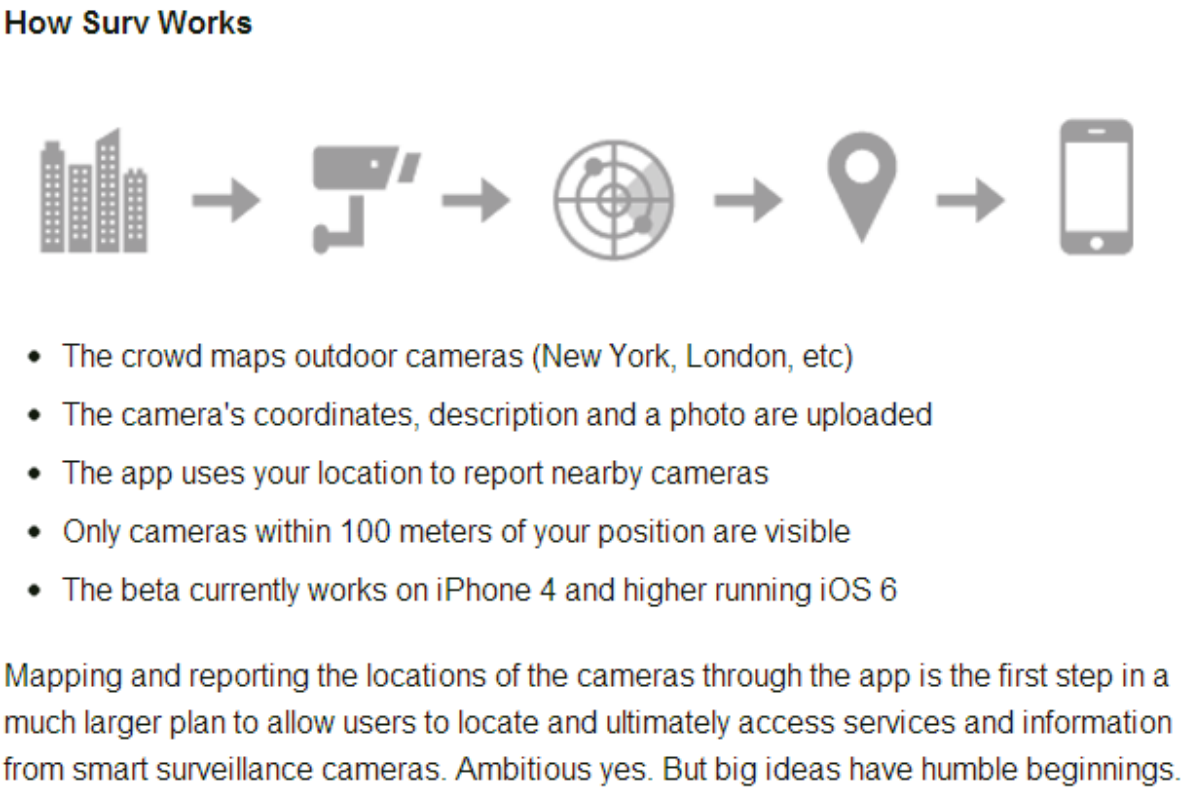

Figure 2: Surv App: How it works.