

# 19

## MITIGATING ASYMMETRIC VISIBILITIES

### Towards a signage code for surveillance camera networks

*Andrew Clement and Joseph Ferenbok*

#### Introduction

CCTV signs govern potential surveillant subjects but also CCTV systems themselves.

*(Lippert 2009)*

Conventional practices surrounding the use of video surveillance in public settings pose a significant challenge to established privacy norms and their underlying civil rights principles. For one, video surveillance tends to be shrouded in secrecy. Operators often keep information about their video surveillance schemes away from both the scheme's subjects and the public more generally. Such camera systems enable others to see you, while remaining opaque to external viewers. The result is a dearth of reliable information about how the captured data is used or repurposed. These practices of obscurity prevent subjects and citizens from making reasonable informed decisions about surveilled spaces, about their regulatory and governing practices and about whether such monitoring is appropriate in the first place. The prevailing asymmetric relationships between surveillers and the surveilled undermine the concept of informed consent as well as ideals of democratic transparency. The growing introduction of automated analysis of visual images, rendering the activities of subjects even more highly visible to surveillant authorities while remaining inscrutable in their own operation, exacerbates this asymmetry (Ferenbok and Clement, this volume). Very seldom are there provisions for adequate public oversight and accountability.

This situation has resulted in part because the growth of surveillance camera networks (SCNs) has outpaced regulatory frameworks governing them in both public and publicly accessible private spaces. Where legal frameworks do exist, they generally are constituted through privacy legislation rather than constitutional or criminal

law (Gras 2004). In the UK, for example, which, following the 1993 murder of James Bulger, became the most prominent publicly funded ‘CCTV state’ (Norris and Armstrong 1999), specific protective legislation only came into effect with the 2000 Data Protection Act (Gras 2004).

One means to help redress this unbalanced power dynamic is comprehensive signage systems. Signage plays an important role in regulating a variety of other potentially risky activities, such as vehicular movement, as in the case of traffic signs, and smoking, via cigarette package labels. In the case of SCN regulation, Lippert notes that:

CCTV signs can govern function creep to the extent signs display a CCTV system’s purposes. In so doing, signs limit cameras from being used for other purposes if subjects gain awareness of new functions and their absence from the text of CCTV signs.

*(Lippert 2009: 516)*

Despite these possibilities, however, when it comes to providing surveillance subjects with meaningful information, signage in many jurisdictions, and Canada in particular, falls short, apparently in large part because there is currently little regulation or oversight (Dawson et al. 2009; Deisman et al. 2009; Lippert 2009). Despite strong arguments that signs are a necessary and integral part of the SCN assemblage (Lippert 2009), the sparse research available suggests that signage implementation, design and oversight vary regionally, but are generally inadequate.

This chapter seeks to help fill these gaps in research and regulation by analysing the shortcomings of current signage practices and offering prototypes of signage schemes that address the key privacy and governance issues. The chapter is divided into two parts. The first looks at prevailing practices around video surveillance signage and the regulations and guidelines that govern them. The second part introduces sample prototypes of three signage schemes that are not only designed to enforce compliance with privacy legislation, but also to help to foster an informed, rights-aware citizenry equipped to hold surveilling organizations to public account. While the focus is mainly on Canadian settings, the findings are broadly applicable to the many other jurisdictions with privacy laws similarly based on fair information practice principles.

## Part I – Prevailing Signage Practices

### 1.1 Current SCN signage in Canada

Anyone looking for video surveillance in Canada’s major metropolitan centres will have little difficulty finding cameras overseeing stores, office block lobbies and shopping malls, and peering onto public sidewalks and parks.<sup>1</sup> Some cameras are quite visible, placed so that it would be hard not to notice them. Most, however, are more discreet – small black domes dotted across ceilings along with

other infrastructural paraphernalia such as lighting, electrical wiring, smoke detectors, sprinklers and ventilation. A first impression is that signs notifying people about the cameras are considerably harder to spot. Most cameras have no signs in their immediate vicinity. Where present, and in contrast to the relatively uniform appearance of the cameras, the signs are varied and far from standardized. Such signs are remarkably uninformative, in that they all give very little indication about what is going on behind the lens. The more fulsome signs tend to be those operated by public bodies. Cameras belonging to private firms appear less likely to be signed and when signs exist, they either exhibit blunt warnings or, less frequently, claim virtues resulting from the cameras such as customer protection and lowered prices. Someone familiar with the Personal Information Privacy and Electronic Documents Act (PIPEDA) could immediately draw the conclusion that many businesses do not comply with Canadian privacy law.

These first impressions are confirmed by other video surveillance researchers in Canada (Deisman et al. 2009; Lippert 2009), as well as preliminary results of a study led by the authors (Clement, Ferenbok and Plataniotis 2010). The following is a sampling of signs displayed at major retail stores in Toronto, Canada. They are part of a much larger corpus of images collected since December 2009 and viewable publicly on the Canadian Surveillance Camera (aka CCTV) Signage Group Flickr page.<sup>2</sup>

In the store from which the photo in Figure 19.1a was taken, the sign(s) are located beside a fire exit – not likely the first place that customers would look for information necessary for informed consent – and one of the signs is obscured by shelving. The stated purposes of the video surveillance in this case are customer protection, ‘low prices and efficient customer service’. However, no information is given about how the video actually helps to protect the customer. For example, is there a live agent or analytic algorithm monitoring the video to provide assistance in case of medical emergencies? The smaller text at the bottom reads: ‘[Tape Recorders] provide the evidence we need to prosecute criminal offenders’, suggesting the purpose of capturing forensic evidence, rather than providing a real-time response for customer protection. The language of the sign implies that lower prices and customer service are supported by reduced shoplifting resulting from the prosecution of offenders. The sign in Figure 19.1a does not mention or make clear whether the information is used for any other purposes, how long the information is retained, with whom it may be shared, who is responsible, whom to contact, or any number of other considerations important to fair information practices.

In the store featured in Figure 19.1b, the sign rationalizes video surveillance by claiming that CCTV monitoring, in conjunction with trained associates, provides ‘customers with the best possible value and [ensures] a safe and secure shopping environment’. However, parallel to the situation in Figure 19.1a, the mechanisms for achieving the stated purposes are not identified. Similarly, in Figure 19.1c, people at that particular retailer are apparently being monitored because the company ‘cares’ about the safety and security of its valued customers. Just as with the other



FIGURE 19.1 Retail video surveillance signs.

two examples, no specific details are provided about the underlying information practices, contrary to the principles of openness and transparency, to established privacy norms and to specific provisions of prevailing privacy law.

The lack of information on existing signs, or the complete absence of signs in many cases, undermines one of the central claims often used to justify video surveillance: that they accomplish deterrence. Although research calls into question arguments about the effectiveness of the cameras as a deterrence measure (Norris, this volume; Deisman et al. 2009), the espoused goal of deterrence should nevertheless provide a strong rationale for visible and effective signage. However, unless individuals know that they are being monitored, the deterrence argument cannot be easily supported. It is ironic then, from a surveillance proponent's perspective, that video surveillance signage is on the whole rare, uninformative, non-compliant with regulations, often located in obscure locations, and mainly text-based and therefore of limited accessibility to non-English-reading populations. The status quo seems to be that informative signs are severely lacking.

### 1.3 Canadian SCN signage law

In Canada, the collection of information for commercial purposes about identifiable individuals is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000, or its provincial counterparts. While PIPEDA makes no explicit reference to video surveillance or related signage, it is clear that all images of a person, regardless of location, if captured with sufficient quality to convey personal information, are subject to PIPEDA. When a video camera captures an image relating to an identifiable 'individual's race, colour, national or ethnic origin, sex, and age' its contents will be 'considered *personal information* under PIPEDA' (2000). PIPEDA obligates companies under Schedule 1, section 5, clause 4.8, the 'Openness Principle', to 'make *readily available to individuals specific information* about its policies and practices relating to the management of personal information' (emphasis added). The first sub-section, 4.8.1, spells out in more detail how this notification is to be provided:

Organizations *shall* be open about their policies and practices with respect to the management of personal information. Individuals *shall* be able to acquire information about an organization's policies and practices without unreasonable effort. This information *shall* be made available in a form that is generally understandable.

(2000, *emphasis added*)

The use of the word 'shall' in both the statement of the Openness Principle and sub-section 4.8.1 is significant, because it indicates a legally enforceable requirement. The standard of 'without unreasonable effort' is also significant in the context of video surveillance operations, since individuals often casually walk into surveilled spaces and thus the information should be easily at hand and quickly understood by people with a diverse range of perceptual and linguistic abilities. People could not reasonably be expected to go to much trouble to seek out information about spaces that they enter casually while going about their everyday affairs.

Further notification requirements are indicated by several other PIPEDA Principles: principle 9 of PIPEDA – Individual Access – states that every citizen has the right to request their personal information and 'shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information'. Principle 2 – Identifying Purposes – states that, 'The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected', and Principle 3 – Consent – states that, 'The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.'<sup>3</sup>

Signs posted in the vicinity of cameras represent an obvious way for organizations to inform individuals about video information collection by surveillance cameras and make available information about their practices. Lippert (2009) notes that 'Signage is the only relatively permanent form of site-specific notification of 'open-

street' CCTV surveillance in Canadian cities' (509). This justifies closer scrutiny of how, where and why surveillance notification is deployed.

### 1.4 Signage guidelines

As there is no specific reference to camera surveillance in privacy legislation, Canadian privacy commissioners have developed several sets of guidelines for video surveillance in public places. In 2001, the Information and Privacy Commissioner of Ontario (IPC) published *Guidelines for Using Video Surveillance Cameras in Public Places* (IPC 2001). These guidelines are aimed at provincial public sector installations and advocate the placement of signs to notify the public when they are entering a surveilled zone. Lippert (2009) suggests that the requirement for signage is significant 'since it demands CCTV signage be a means of notifying the citizenry not merely of a surveillance camera's presence nearby, but also *why* it is in place, *how* more information about its purposes can be gained, and *how* a complaint can be initiated if necessary' (2009: 509). However, the guidelines are 'intended to assist organizations' with the deployment of their surveillance systems and are not binding or enforceable.

The IPC Guidelines offer public bodies in Ontario this template for a video surveillance sign:

Attention

This Area May Be Monitored by Video Surveillance Cameras.

(CCTV)

The personal information collected by the use of the CCTV at this site is collected under the authority of (an Act) and (by-law). This information is used for the purpose of promoting public safety and reduction of crime at this site.

Any questions about this collection can be directed to the Manager of (Department) at (phone number), (City Hall address) (e-mail).

(IPC 2001: Appendix A)

This template has seen adoption in public organizations such as the Toronto Transit Commission and Toronto City Hall. These signs, however, have several key limitations. As Lippert (2009) has noted, the above example is typical of textual signs that systematically exclude the illiterate, visually impaired, those less likely to be able to read English (or French) like tourists, immigrants, and youth. But perhaps equally as troublesome as the disenfranchisement of various groups is the lack of any mechanism for oversight and regulation. The lack of signage that adequately communicates complaint procedures 'helps explain why from 2001–2007 the Ontario privacy commission received only one complaint about "open-street" CCTV and not a single legal order concerning "open-street" CCTV signage was issued' (Lippert 2009: 514). Although the signage template above superficially informs sign readers that subjects may be monitored, it gives no indication of the type of

monitoring employed. Nor are subjects told if the monitoring is live, in real-time, by human agents, or mediated by computers. Furthermore, the template says nothing about system capabilities, storage duration, third-party access, emergency response, and so on. Because the template is silent on any specific capability of the SCN it does not require the organization to update or revise the wording when system practices or technologies change. This means, for example, that there will be nothing to alert subjects when video analytic techniques such as facial recognition are incorporated in the behind-the-lens processing.

The Office of the Privacy Commissioner of Canada (OPC) has also issued three sets of video surveillance guidelines. The first, in 2006, is *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities*. Recognizing that ‘Video surveillance of public places subjects everyone to scrutiny, regardless of whether they have done anything to arouse suspicion’, the OPC stresses in guideline 7:

The public should be informed with clearly written signs at the perimeter of surveillance areas, which advise that the area is or may be under surveillance, and indicate who is responsible for the surveillance, including who is responsible for compliance with privacy principles, and who can be contacted to answer questions or provide information about the system.

(OPC 2006)

Another set of *Guidelines for Overt Video Surveillance in the Private Sector* (OPC 2008), developed jointly with British Columbia and Alberta Commissioners, relates more directly to PIPEDA. In the FAQ section they note:

**Q.** Should we post signs that there are cameras in operation?

**A.** Yes. Most privacy laws require the organization conducting video surveillance to post a clear and understandable notice about the use of cameras on its premises to individuals whose images might be captured by them, *before* these individuals enter the premises. This gives people the option of not entering the premises if they object to the surveillance. Signs should include a contact in case individuals have questions or if they want access to images related to them.

(OPC 2008, *emphasis in original*)

The emphasis on information that allows citizens to make informed decisions and provide informed consent when entering surveilled spaces is particularly significant to the discussion of signage here. Research findings discussed below suggest that the current practices do not facilitate informed consent.

Finally, in 2009, the OPC published *Guidance on Covert Video Surveillance in the Private Sector* (OPC 2009). Particularly relevant to the present discussion is that the guidelines consider ‘video surveillance to be covert when the individual is not made

aware of being watched', and that, while justifiable under some circumstances, 'covert video surveillance must be considered only in the most limited cases' (OPC 2009), pointing again to the importance and significance of location-based signage at the point of surveillance. In short, these guidelines all draw on principles of transparency and openness, reinforcing the privacy principles underlining PIPEDA.

### 1.5 Signage regimes in other jurisdictions

The UK is often used to exemplify the modern surveillance state (Norris and Armstrong 1999). According to Cole (2004), 'the expansion of surveillance in the UK took place with little or no regulation until March 2000, when the Data Protection Act came into force' (2004: 44). The UK code, in keeping with the First Data Protection Principle, requires signs to inform the public that they are entering a surveillance zone. The code also specifies the information that should be contained on the sign. As Cole (2004) reports, a sign should indicate the person or organization responsible for the surveillance, and the purpose of the surveillance, and provide contact information of someone who can provide details about the surveillance scheme. This is essentially just the same information as specified in the IPC guidelines, which, as discussed above, lack many other necessary elements for proper informed consent. However, as research by Lizar and Potter (this volume) indicates, compliance with even this minimal standard is far from universal.

Gras (2004) offers a comparison of CCTV signage across Europe. In 2004, she noted that, 'Denmark certainly has stronger regulation than Britain. CCTV surveillance is generally forbidden there' (Gras 2004). As Norris (this volume) notes, CCTV was slower to penetrate the Scandinavian countries, although some public cameras have been introduced more recently in Denmark and its neighbours. In Germany, significant regulation of CCTV surveillance also exists. German regulations stress proportionality and attempt to weigh the tension between property rights and the rights of individuals. This system of regulation appears to force parties (such as the police) to justify the deployment and continued use of surveillance systems. Gras (2004: 220) notes,

secret CCTV would be permissible if used to take immediate steps and to prevent crime. Where this purpose is not served, individual privacy is more important. Where CCTV is used more as a form of entrapment to secure evidence, the courts will declare this use unfair and illegal, if no warning of potential surveillance is given.

If this were to occur it might provide corporations the impetus to rethink their video surveillance policies.

Although covert surveillance, without signage or notification, would thus be considered inadmissible or illegal in Germany, legal regulation seems to use *ex-ante* legal thinking by suggesting that 'secret CCTV would be permissible if used to take immediate steps and to prevent crime' (Gras 2004: 220). Signage, therefore, is seen as



significantly ‘lowering the level of interference with constitutional rights CCTV surveillance is seen as causing’ (Gras 2004: 225). This position implies that ‘crime prevention’ requires live monitoring, to stop an imminent crime from happening. This argument suggests that in order for an operator in Germany to claim crime prevention as a purpose of a SCN, the system must include the possibility of immediate intervention. This argument is even stronger when applied to a stated purpose of ‘public safety’. If an operator states the purpose of a SCN installation is, in part, ‘public safety’ then they have to have real-time (human and/or automated) viewing and a capacity for timely intervention. Extending this to our purposes, any proposed signage scheme, with purposes of either ‘public safety’ or ‘crime prevention’ should coincide with real-time monitoring.<sup>4</sup> Conversely, SCN operators cannot adequately justify claims of ‘crime prevention’ or ‘public safety’ as purposes with systems that only record.

Similar to the regulation in Germany, ‘the law in France, Sweden and the Netherlands requires that attention be drawn to CCTV surveillance by signs placed outside of the surveillance area so that a person be made aware of entering it’ (225). The placement of signage outside areas under surveillance speaks to the idea of implied consent, or that a citizen, being made aware of the surveillance, is thereby given the chance to choose whether to enter the space or not. Of course this point remains somewhat contentious, not only because the legal concept of consent is complicated, but also because the cost and inconvenience of avoiding some surveillance zones is arguably unacceptably high: for example, those who need to travel by train for work are given little choice but to enter the surveilled space of a railway station, even if they do not consent to the surveillance there.

### 1.6 Summary and implications

The above discussion demonstrates that in Canada there is a clear lack of appropriate video surveillance signage, oversight and regulation. This inadequate signage is a serious, publicly visible contravention of fair information practices as well as Canadian privacy guidelines and legislation, particularly that covering the private sector. Other jurisdictions appear to be in a similar position, though in some cases surveillance practices and signage requirements are more rigorously defined and enforced. This situation is exacerbated by the absence of public debate and discussion around surveillance camera issues. The need for more public engagement is clearly evident; as is the need for more open and transparent practices supported by signage that attempts to mitigate the existing asymmetry in the surveillance of public spaces.

## Part II – Towards a citizens’ rights signage scheme

Supported by the motivations, principles and practices discussed above, the second part of this chapter explores our proposed video surveillance signage schemes. It looks at how other signage practices and domains have informed our design, sketches a basic use scenario that the principal scheme aims to address, outlines the

main features of the scheme and presents our sample prototype signs intended for various use contexts.

## 2.1 Signage regimes in other domains

There are several distinct, although not necessarily mutually exclusive, categories of signs: orientational, informational, directional, identificational, ornamental and statutory or regulatory signage (Sims 1991). Iconic signs are generally more accessible than text-based signs for the greater population. Visual cues offer quick access to information once the icons are commonly recognizable, and with good design, icons are more easily learned. To make images more accessible designers often use icons. Simple icons generally use high contrast to make signs more legible from a distance. But there is a danger with over-simplification, as it can undermine the goals of the signage system leading to vague or muddled readings. Misinterpretation can be mitigated by using combinations of icons and written text. Good design also allows for communication of complex information across cultures, languages and varying levels of literacy.

Signage must take into account target populations, and especially populations that may be in danger of becoming disenfranchised by the systems. For example, signage that is not supplemented by other modes of communication becomes inaccessible for the visually impaired. Signs that are text-based may present challenges for illiterate or non-English/French reading audiences. Commonly, good sign design considers a number of key general and contextual factors. Primary considerations include legibility, colour, material, size, location, positioning, background and ambient lighting (Sims 1991). Legibility often includes concerns such as letterform, contrast and visibility at a distance. Colour has significant symbolic meaning that is often culturally and contextually specific. Further issues include: Is the copy readable? Does the sign answer the design brief? Is it highly legible? Is it appropriate for the target audience? Does it promote the 'right' image? Is the information given a proper degree of visual emphasis? Does it comply with signage legislation? etc. (Sims 1991). These questions are useful not only for the design process but also for subsequent evaluation of the signage. Within Canada, and more generally around the globe, video surveillance signage is varied and far from user-centric, so other, better-developed signage domains can likely offer some valuable lessons.

## 2.2 Signage characteristics

Cole (2004) classifies signs based, at least in part, on their mode of address. Or, put another way, signs can be analysed according to whom they seem to address or hail. The 'dispassionate' sign attempts to convey the presence of surveillance as simply a matter of fact; the 'inclusionary' sign attempts to hail the 'good' citizenry by including them in promises of safety, security and lower prices; 'exclusionary' signs attempt to repel the other, the criminal or undesirable subset of the population

to 'warn' them about the presence and potential repercussions of video surveillance; some signs are double-coded targeting both desirable and undesirable populations simultaneously. Cole (2004) argues that with its ideological targeting of both the 'public' and the 'other', 'signage now conspires with the surveillance itself to amplify the panoptical effect that many have [been solely] ascribed to CCTV' (2004: 14).

Our aim is to develop a signage scheme that principally hails the surveilled subject as a rightful citizen, in notable contrast to the more typical 'suspicious intruder' (exclusionary) or neo-liberal 'informed consumer' (inclusionary) approaches that Lippert (2009) highlights. We do this in terms of signage content by supplementing the information required for the informed consenting consumer with resources for exercising their rights and for holding the surveillance operators more accountable for their practices. In particular, we provide access to more comprehensive details of the surveillance scheme as a whole, reminders of citizen rights, the procedures for filing complaints and the means for connecting with others who may have similar concerns.

For our visual presentation purposes, we emphasize a few key criteria in our proposed signage scheme: legibility, colour, visibility and location. To promote legibility, we employ high-contrast backgrounds and sans serif fonts that are large enough to be seen from a distance. Following the Vienna Convention on Road Signs and Signals (1968), our signs mainly use black or red text and symbols on yellow or white grounds. We also take into consideration the location and positioning of the signs. If the signs are located by fire exits or obscured by shelving (see Figure 19.1a), they may merely serve as an ironic, theatrical nod towards compliance. Physical signs are best placed at eye level starting just beyond the outer edge of a surveillance zone, and positioned strategically within it.

So we envision two particular types of situational contexts: orientational/informational and statutory/regulatory. The first situation, orientational/informational, requires signage that provides just-in-time information that allows people to determine how to orient themselves in a particular surveillance context. This category, like road signs, requires quick, legible and digestible information at the periphery of a surveillance area that provides useful information to someone about to enter. For those who wish to obtain 'deeper' information about the surveillance system and its compliance and governance, the statutory or regulatory signage includes more extensive information about contacts, policies and capacities of the system. There will be fewer of these signs, but their full content should also be readily available via the web.

### 2.3 Basic use scenario

We base the design of our surveillance camera network signage scheme on the scenario of a person walking along a public street or a private retail space normally accessible to the public, who encounters a commercially operated video surveillance zone. This provides a good starting point for analysis, as this is the most common site for people to come under video surveillance.

Anyone concerned for their privacy or safety is immediately faced with the decision of whether to proceed into or avoid the surveilled area. She could plausibly ask many of the following questions: Am I safe here? Who is operating the cameras and responsible for this operation? Can they be trusted (i.e. are they a legitimate operator, do they have a legal authority to operate, do they have a good record of legal compliance and civil respect)? What's the purpose of the cameras? What can the cameras see? What is the scope of the surveilled area? When am I inside the area and when am I beyond it?

She may also want to know more about the nature of the surveillance: Is the monitoring live or automated? Is someone watching right now? Who are they? Where are they? Are they trained and competent? Will I get help if something adverse happens to me (e.g. fall down, feel ill, get mugged, etc.)? Whom do they report to? Am I being recorded? Who views the recordings? What is done with them? How might I be affected?

It can be reasonably expected, based on the Openness Principle, that the operator of the SCN should readily provide answers to any of these questions. PIPEDA in particular, as noted above, requires organizations to 'make readily available to individuals specific information about its policies and practices relating to the management of personal information'. Furthermore, 'individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable' (2000).

## 2.4 Proposed signage schemes

Applying the principles of openness and informed consent to this use scenario helps determine the main features of our proposed signage schemes that, as discussed above, hail the surveillance subject as a rightful citizen. There are two distinct, but consistent, knowledge interests that need to be served. The first is that an individual data subject (e.g. consumer) should be in a position to readily find answers to the questions posed in the scenario above. In particular, such a person should be forewarned of an upcoming surveillance area and its characteristics. Signs should be legible at walking speed and readily provide the individual with sufficient detail to make a rapid, informed decision about whether to enter the space, how to behave within it, and where to turn for assistance. If the individual enters the surveillance zone, she should receive reminders of the basic features of the surveillance while she remains within the zone. If she wants to learn more about the surveillance operation, she should have little difficulty in finding signs that provide full statutorily required details. These signs serve a dual purpose in the sense that they also help regulate the operator by enforcing the public disclosure of video surveillance capacities, purposes and infrastructure as a whole.

A second public interest served by organizational openness and transparency is that of good governance. Citizens seeking to exercise their democratic rights

effectively, whether acting individually or collectively through civil society organizations, also need to be well-informed about how organizations process personal (visual) data – the risks, the safeguards, and the opportunities as well as the remedial possibilities. Likely the best way to provide this information is through a website containing the full statutorily required details, and that facilitate the making of formal requests to the responsible organization where further information is required.

While our principal focus is on the signage that an SCN owner/operator should post, there are occasions when the regulator may need to post their own signs to alert (potential) surveillance subjects of the legal status of the operation. Other parties may also post signs in a more ad hoc fashion to draw attention to concerns they have about the surveillance operations. Therefore our proposed scheme includes not only the signage posted by operators, but also signage posted by regulatory enforcement agents as well as signs posted by individual citizens or civil society groups concerned with public policy issues and non-compliant operators. We consider prototypical examples of these three types of sign in turn.

## 2.5 Operator-posted notification

The principal means to address the two main knowledge interests is to require SCN operators to post a variety of situationally appropriate signs around the periphery of and throughout their surveillance zones. We propose four specific types of location-specific, operator-posted physical signs: surveillance border notification, surveilled area signs, camera labels and full disclosure signs. In addition to these we propose an operator-hosted online portal accessible via a web or smartphone app interface. After enumerating the various icons and their meanings used in the signage scheme, we describe each of these sign types in the order that a surveillance subject will most likely encounter them.

### *Surveillance camera network signage icons*

In order rapidly to convey key information about the purposes and operational characteristics of particular surveillance camera network operations, we have developed a set of high-visibility icons to be used consistently throughout the signage scheme (see Figure 19.2).

This is a partial list covering only some of the more common surveillance scheme characteristics. Other icons in development include those to alert surveillance subjects of various other purposes and video analytics capabilities (e.g. facial/body recognition, facial/body encryption and facial/body blurring).

### *Surveillance border notification*

The first notification of a video surveillance operation that a person encounters should be a border sign like that shown in Figure 19.3. It compactly depicts all the key informational elements on which to make an informed decision about whether



## Toronto City University

The area indicated in the accompanying map is monitored by a Video Surveillance Network (VSN, aka CCTV) under the control of the University of Toronto and operated by Chubb, and is in compliance with the relevant regulations of the Office of the Privacy Commissioner.



# THIS AREA IS UNDER VIDEO SURVEILLANCE



### Crime Prevention/Prosecution

Criminal investigation and prosecution - In the case of suspected criminal activity, the incident will be reported to law enforcement authorities, who may request access to stored images.



### Public Safety

Emergency response in case of a personal safety incident



### 24hr Live Monitoring

The video images are monitored by trained staff 24 hours/day, 7 days a week.



### 3 day Image Storage

The stored video images are deleted after 3 days, except when there is duly authorized investigation of an reported incident in which case they are retained only as long as needed for the investigation. All such retentions are logged and reported in the annual audits.



### Face Recognition

No automated facial recognition



### Face Blurring



### Image Encryption

To preserve anonymity, human body images are encrypted before storage, and only de-encrypted in case of investigation of serious incident by senior law enforcement authorities. All such de-anonymizations are logged and reported in the annual audits.



To report an incident call 800-555-9999. If an emergency, call 911. To view our privacy and video surveillance policies, request a copy of your personal images, register a complaint, review our annual audits or ask a question, visit: <http://organization.ca/video-surveillance>. Questions can also be directed to the Chief Privacy Officer, phone 800-555-1000 or [PrivacyOffice@organization.com](mailto:PrivacyOffice@organization.com). If this does not produce a satisfactory response, you may register a complaint with the Office of Privacy Commissioner - <http://opc.ca>

FIGURE 19.2 Index of icons.

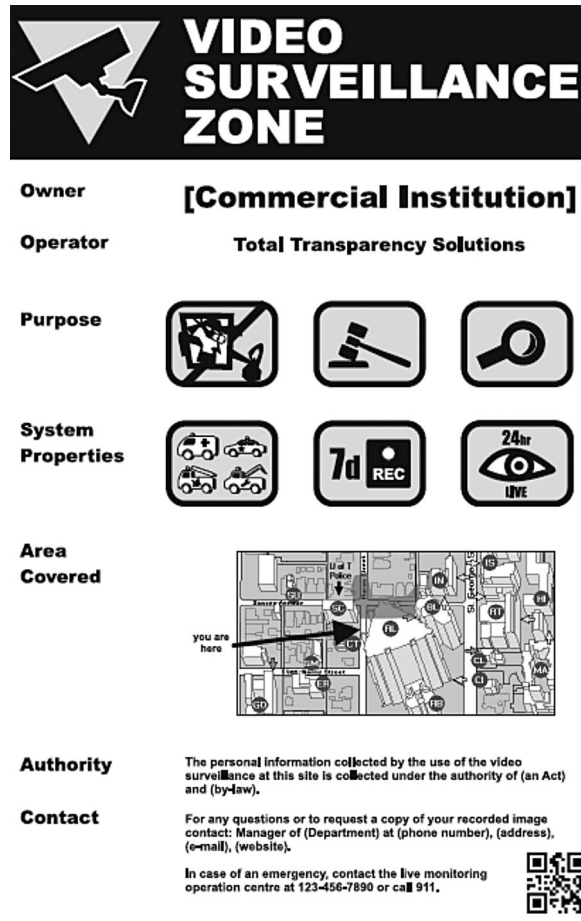


FIGURE 19.3 Sample operator-posted border sign.

or not to enter a surveilled area. In particular, it contains the following elements in text and/or iconic form:

- Organization(s) responsible

- Purposes/justification for scheme – crime detection, forensic analysis, prosecution?

- Properties of the surveillance scheme – emergency response, seven-day recording, 24/7 live monitoring

- Area covered by the surveillance scheme

- Authority to operate

- Responsible person, with contact details

- Procedure for accessing or correcting one's personal record

- Oversight of scheme – independent third-party oversight

- 2D barcode providing link to surveillance scheme informational portal website

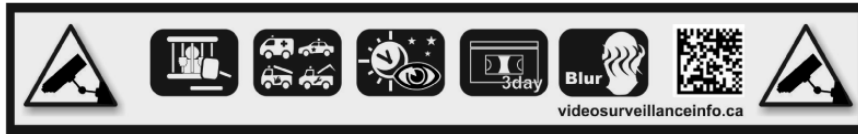


FIGURE 19.4 Sample operator-posted border stripe.

In our SCN signage scheme, this border sign may be supplemented by yellow stripe with embedded logos and icons that depict the ownership, operator, purposes and properties of the surveillance installation, as shown in Figure 19.4. This strip would be applied to existing surfaces (e.g. sidewalks and walls) along the periphery of the surveilled area. Border and area notification should also be done digitally: for example, a mobile app designed for the purpose tells the subject when approaching a virtual ‘yellow stripe’.

### Area signs

Small signs scattered throughout the surveilled area would incorporate key icons and contact information. These signs would be placed along trafficked paths and near gathering points within the surveilled area. The image in Figure 19.5 provides a sample of what this type of sign might look like.

### Camera labels

Each surveillance camera should have its own identification sign that gives the unique camera ID and key specifications (recording and live monitoring) of the



FIGURE 19.5 Sample operator-posted surveillance area sign.



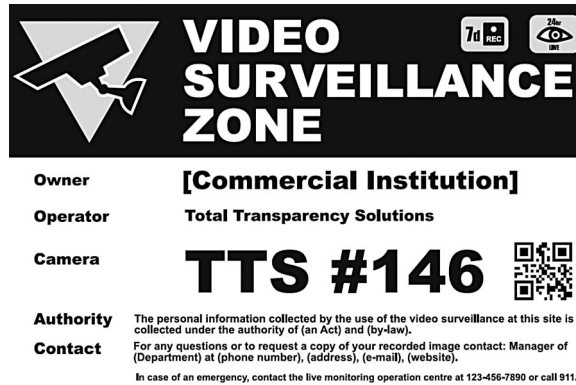


FIGURE 19.6 Sample operator-posted surveillance camera sign.

camera. The 2D barcode links the camera ID to the portal website where more information about the camera and the SCN is provided (see Figure 19.6).

### *Full disclosure signs*

Placed at prominent points of entrance are larger information signs with full statutorily required details about the surveillance scheme.

These posters incorporate in one place all the information about icons, explanations, coverage map, regulations, authority, access procedures and contact info contained in the various other signs.

### *Portal website*

Integrating all of these forms of signage and ensuring transparent communication will be an online interface that provides full, up-to-date disclosure, including policy documents, annual reports and independent audits about the SCN.

Any such scheme depends on clear, intuitively accessible icons, sensitive to context and culture, that have been tested and iteratively developed. The design of any such system requires incremental refinements based on feedback from the various stakeholders.

## **2.6 Regulatory enforcement agent-posted signage**

In many areas involving public safety or protection, it is common for regulatory or independent certification bodies to require enterprises to post signage of their own creation indicating that the specified operation complies with official standards. Examples include elevators, commercial weight scales, fire extinguishers, and many other devices in common usage, which typically display a certificate of compliance. Often included in the signage is an expiry date, by which time some form

of examination and recertification is needed. There is currently no such certification requirement for surveillance camera networks, at least in Canada, but it is not inconceivable that if the widespread non-compliance of current video surveillance with privacy regulations and guidelines becomes better known and public pressure is brought to bear, then the current regulatory bodies will become more active in this area. While this may not be an immediate prospect, it might be helpful to suggest what a model of greater regulatory oversight would involve. One approach is showing samples of the official signage that operators need to display. The signage scheme of the Food Premises Inspection and Disclosure System at the City of Toronto Health Department, better known as DineSafe, provides such an example. The most publicly visible indicator of the inspection and certification programme is the prominent status sign that appears in every restaurant's front window alerting prospective diners of the current state of compliance with the Ontario Food Premises Regulation. A green PASS sign indicates a satisfactory inspection; a yellow CONDITIONAL PASS sign indicates a recent health inspection that found 'Significant Infractions', needing to be corrected within 24–48 hours; and a red CLOSED sign indicates that one or more 'Crucial Infractions' were observed during an inspection, and the establishment ordered to close. An extensive website<sup>5</sup> explains the signage as well as reports on the inspection and compliance history of every restaurant in Toronto.

Taking this as a model and applying it to private sector surveillance camera networks suggests the relevant Privacy Commissioner would make periodic inspections of video surveillance operations and require the prominent posting of one of the following three compliance status indicators (see Figure 19.7):

Pass (green) – meets the relevant privacy law requirements

Probation (yellow) – doesn't meet the relevant privacy law requirements, but is given a certain period to meet the standard before being shut down  
Stopped (red)

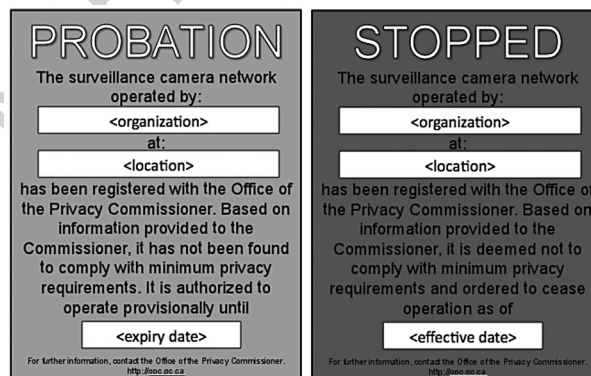


FIGURE 19.7 Sample regulator-posted compliance status signs.

following a probationary period, or in the case of severe violation of the privacy standards, the scheme is ordered to cease operations.

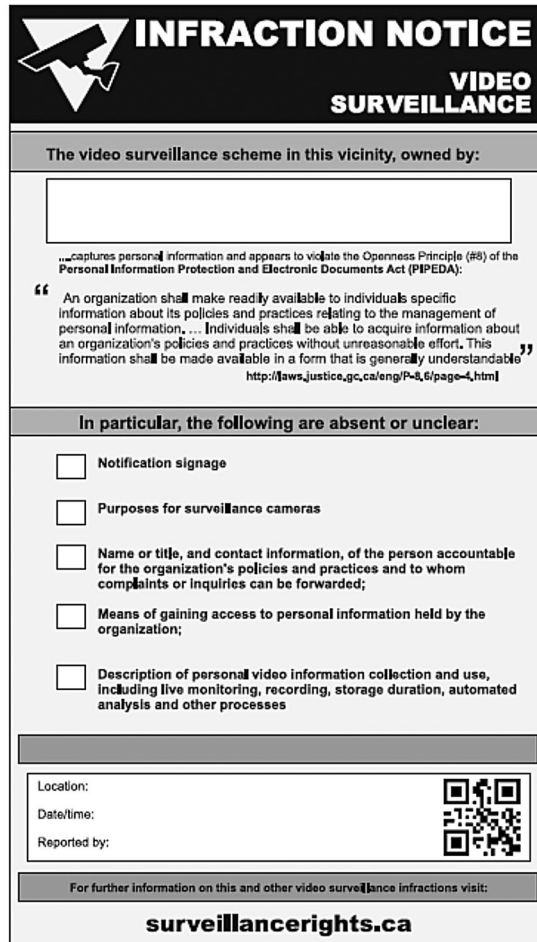
As with DineSafe, these signs could be integrated with a website that tracks (non)compliance of surveillance camera network operators, enabling relatively easier public oversight that would help mitigate the current asymmetries of visibility.

While the Canadian privacy commissioners currently have audit powers that they could use to conduct inspections of video surveillance operations, they would also need considerable additional resources to carry out inspections on a systematic basis. They could seek an increase in the funding they receive from Parliament, perhaps through a licence fee for video surveillance operations. While such a fee would be a small fraction of the cost of the installation and operation of a surveillance camera network, businesses would certainly actively resist the additional expense, as well as the heightened regulatory oversight more generally. Given the current neo-liberal political climate, it should be expected that they would receive political support in opposing this stiffer form of regulation. It might need major popular resistance to the current video surveillance practices to overcome these obstacles. Suffice to say, such measures are not imminent. However, this does not mean there is nothing that can be done along these lines in terms of greater external compliance monitoring and notification. We turn now to the possibility of a citizen-initiated inspection and signage scheme.

## 2.7 Citizen-posted signs

While most of any surveillance camera network operation is out of sight, it is often the case that some cameras are visible, at least alerting passersby to the existence of the operation. It is then relatively easily to determine whether there is signage, and if so, whether it meets the standards specified in the privacy commissioners' guidelines. With modest instruction in the requirements of PIPEDA, anyone interested could determine whether the signage associated with a specific video surveillance operation is minimally PIPEDA-compliant or not. This provides the basis for an individual to file a complaint with the appropriate privacy commissioner. To give this more visibility and weight, the complainant could alert others by posting their own sign, as seen in Figure 19.8. Based on the bright yellow parking tickets dreaded by Toronto drivers, this 'Video Surveillance Infraction Notice' identifies the organization responsible, the time, date and place of the infraction, and the specific shortcomings of the signage. Details of the infraction, and preferably a photo of the notice, the issuer and the premises, could be posted to a website similar to the DineSafe site or the Flickr group mentioned above.

The accessibility of an independently maintained website with details of SCN operations and their apparent compliance status by the growing number of smartphones offers a new way of informing people of the proximity to and characteristics of video surveillance zones. Those people with GPS-enabled smartphones with a specially designed application could be automatically alerted by their device as they



**INFRACTION NOTICE**  
**VIDEO SURVEILLANCE**

The video surveillance scheme in this vicinity, owned by:


...captures personal information and appears to violate the Openness Principle (#8) of the Personal Information Protection and Electronic Documents Act (PIPEDA):

“ An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information, ... Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable ”

<http://laws.justice.gc.ca/eng/P-86/page-4.html>

In particular, the following are absent or unclear:

- ☐ Notification signage
- ☐ Purposes for surveillance cameras
- ☐ Name or title, and contact information, of the person accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- ☐ Means of gaining access to personal information held by the organization;
- ☐ Description of personal video information collection and use, including live monitoring, recording, storage duration, automated analysis and other processes

Location: 

Date/time:

Reported by:

For further information on this and other video surveillance infractions visit:

**surveillancerights.ca**

FIGURE 19.8 Sample Video Surveillance Infraction Notice.

approach an SCN operation that had previously been registered in the database (see Figure 19.9). Where physical signs have been posted with the 2D barcodes, as shown in the various sample images above, the app could read the barcode and thereby expedite access to the information about the particular installation. The app would also encourage contributions to the database through the uploading of photos and other relevant information. In this way, the signage would become usefully hybridized across physical and digital media and offer a means for public ‘crowdsourcing’ of (non)compliance reporting data as well as serve as an educational and mobilizing medium.

The specific design features of this hybridized signage scheme will be important factors in attracting and maintaining the active voluntary participation needed to achieve these oversight, educational and political purposes. This will require



**FIGURE 19.9** Sample Civic alert signs on GPS smartphone.

iterative prototyping with interested individuals, as well as a strategy for wider public involvement.

## 2.8 Future work

The signage schemes sketched above are still at a rudimentary, conceptual, prototype stage. The images presented here are intended mainly as an illustration of a particular approach to the regulation of SCNs, one that stresses making their presence and operational characteristics more publicly visible. Clearly much work remains to be done to give substance to the proposed approach. A next stage will be to test these prototypes in workshop and field settings. We will be interested to see how people react to the potential value of making SCNs more legible and accountable, as well as to the specific design features, such as the readability of the signs and the icons in particular. We also want to see how retailers and other private sector operators react to the possibility of posting much more explicit signs about their SCN operations. While we anticipate that most will not welcome our approach, based on preliminary findings of fieldwork already underway, we have good reason to believe we will find a few smaller retail operations that would be willing to try out our prototype signs. We will assess how people interact with the signs, and use the feedback to refine the scheme. This will likely require several iterations until we gain a clear sense of what is workable.

It would also be interesting to see how the proposed signage scheme fits in a range of settings and jurisdictions, which, as we have seen above, vary considerably in terms of rules and cultural norms. While the signage scheme has been designed specifically with the Canadian commercial SCNs and legislation in mind, it should be adaptable to other jurisdictions, given that they suffer similar problems of

inadequate signage, and that the PIPEDA legislation is considered similar to the EU Data Protection Directive.

## Conclusion

The ongoing rapid expansion of video surveillance largely unfettered by effective regulation and public oversight poses a significant challenge to privacy and other civil liberties. The need for action is made more urgent as operators incorporate increasingly powerful digital techniques, such as video analytics (see Ferenbok and Clement, this volume), behind the scenes. This situation calls on those of us concerned with this development to consider the various means to intervene in the process and ameliorate the likely consequences. There may be no turning back the tidal wave of video surveillance systems proliferating across public and quasi-public spaces, but how the surveillance technologies and practices are regulated, and how individuals can learn and exercise their rights in relation to them, still remain to be negotiated between citizens, policy-makers, politicians and surveillers.

Lippert (2009) has identified signage as one aspect of video surveillance assemblages (Haggerty and Ericson 2000) that can help regulate not only surveillance subjects, but also the surveillance assemblages themselves. Signs, both physical and digital, may prove one point of intervention that can inform citizens of their rights as well as bring operators to account.

This chapter has considered what a privacy-oriented, rightful-citizen signage scheme might look like in a Canadian context. We examined how legislation such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and related guidelines can inform video surveillance signage in public spaces. From this analysis we sketched the key elements that a national video surveillance scheme should include and proposed illustrative prototypes to show how such a scheme might appear. Our signage scheme is, at this early conceptual stage, primarily a design probe that we hope will stimulate discussion about signage as a tool for promoting greater transparency and public accountability of video surveillance practices and technologies. The proposed signage code draws on existing conventions of other sign design domains – such as road traffic and food – that have been adapted for displaying key characteristics of surveillance schemes in everyday, street-level situations.

The proposed scheme has a number of advantages. At the very least, signs make surveillance more visible. The increased visibility may make the surveillance more effective in deterrence where deployed legitimately, while raising the profile of surveillance of public spaces as a broader policy issue. The proposed signs provide people with useful, actionable information about surveilled spaces. The operator-posted signs attempt to communicate complex information in a concise and timely way to surveillance subjects, allowing them to know, for example, what type of response they are liable to get in an emergency and how long their information is kept. The signage scheme is designed to be inclusive to

multicultural, multilingual and even illiterate audiences. The signage also requires retailers, for example, to be more transparent to their customers, and therefore increases the responsibility of the surveillor for the installation and operation of camera surveillance. The authors understand that the proposed signage scheme may have its own limitations and is bound by the limitations of signage schemes more generally. However, in addition to serving as a public didactic tool, it is a first volley at information design and something for policy-makers to criticize, overhaul and implement.

Of course, no matter how comprehensive and widely implemented a signage scheme may be, it provides no guarantee for what operators actually do and how they affect surveillance subjects. While many operators will likely resist any requirement to post more informative signs, if they are forced to do so, the measure will not be difficult or expensive, at least in comparison to the resources required for SCN installation and operation itself. The more intractable organizational processes could continue largely unchanged, unless the signage scheme is combined with more rigorous independent auditing, reporting and disciplining of internal surveillance operations. In this light, we envision our signage schemes as just one strand of a broader public policy discussion surrounding video surveillance practices. In the absence of any more promising intervention strategy, a citizen-centred video surveillance signage scheme as sketched here may provide an approach to mitigating the current asymmetries of visibility and power.

## Notes

- 1 In Vancouver, volunteers organized by the Vancouver Public Space Network mapped over 2,000 cameras in the central business district and surrounding areas. See: <<http://www.vancouverpublicspace.ca/index.php?page=cctv>> 'Volunteers map Vancouver's public surveillance cameras' and *Vancouver Sun*, 23 August 2009: <<http://www.vancouversun.com/Volunteers+Vancouver+public+surveillance+cameras/1922426/story.html>>.
- 2 See: <<http://www.flickr.com/groups/1233129@N25/>>.
- 3 Office of the Privacy Commissioner, Privacy Principles: <[http://www.priv.gc.ca/leg\\_c/p\\_principle\\_e.cfm](http://www.priv.gc.ca/leg_c/p_principle_e.cfm)>.
- 4 Some may argue that the deterrence effect of record-only video surveillance can constitute a form of crime prevention. However, given the very weak evidence for such deterrent effect, the onus should be on the operator to demonstrate convincingly the deterrence effect of their particular SCN.
- 5 See: <<http://app.toronto.ca/food2/DineSafeMain>>.

## References

- Clement, A., Ferenbok, J. and Plataniotis, K. (2010) "'Smart" Private Eyes in Public Places? Video Surveillance Analytics', Toronto: Office of the Privacy Commissioner of Canada.
- Dawson, D., Derby, P., Doyle, A., Fonio, C., Huey, L., Johnson, M., Leman Langlois, S., Lippert, R., Lyon, D., Pratte, A.-M., Smith, E., Walby, K. and Wilkinson, B. (2009) 'A Report on Camera Surveillance in Canada: Part Two', Kingston: Queens University.
- Deisman, W., Derby, P., Doyle, A., Leman Langlois, S., Lippert, R., Lyon, D., Pridmore,

- J., Smith, E., Walby, K. and Whitson J. (2009) 'A Report on Camera Surveillance in Canada: Part One', Surveillance Camera Awareness Network (SCAN).
- Gras, M.L. (2004) 'The Legal Regulation of CCTV in Europe', *Surveillance & Society*, 2(2/3).
- Lippert, R. (2009) 'Signs of the Surveillant Assemblage: Privacy Regulation, Urban CCTV, and Governmentality', *Social & Legal Studies*, 2009(18): 505–22.
- Norris, C. and Armstrong, G. (1999) *The Maximum Surveillance Society: the Rise of CCTV*, Oxford: Berg.
- Office of the Privacy Commissioner & BC and Alberta Commissioners Guidelines for Overt Video Surveillance in the Private Sector, March 2008.
- Peacock, C., Goode, A. and Brett, A. (2004) 'Automatic forensic face recognition from digital images', *Science and Justice*, 44(1): 29–34.
- Sims, M. (1991) *Sign design: graphics, materials, techniques*, London: Thames and Hudson.

### Documents cited

- 'Personal Information Privacy and Electronic Documents Act'. Canada, 2000.
- 'OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities (March 2006)'. Online. Available HTTP: <[http://www.priv.gc.ca/information/guide/vs\\_060301\\_e.cfm](http://www.priv.gc.ca/information/guide/vs_060301_e.cfm)> (accessed 23 August 2010).