

# **Minimal Privacy Compliance Standard for Canadian video surveillance installations**

Draft – January 16, 2013 – Comments welcome

Andrew Clement <[andrew.clement@utoronto.ca](mailto:andrew.clement@utoronto.ca)>

This document specifies minimum privacy compliance standards for video surveillance installations in Canada. It provides the basis for assessing the eligibility of candidates for receiving the \$100 reward offered “to the first person to bring a minimally compliant private sector installation to [the] attention” of the Surveillance Rights project.<sup>i</sup>

This standard is designed to be uniform for all video surveillance installations whether operated by government agencies or for commercial purposes, regardless of location. It is based primarily on the *Guidelines for Overt Video Surveillance in the Private Sector* posted by the Office of the Privacy Commissioner of Canada, supplemented by provincial guidelines where these exist.<sup>ii</sup> These guidelines are synthesized from the various privacy laws in Canada.<sup>iii</sup>

This specification mainly addresses signage, but following the *Guidelines*, also considers other aspects of the video surveillance installation that determine minimal compliance.

## **Signage**

A video surveillance installation refers to one or more surveillance cameras (and ancillary devices) in close proximity to each other managed together under a common authority. For an installation to be minimally compliant it is necessary, but not sufficient, to post signs informing passersby of the presence of video surveillance in the vicinity.

Signage compliance is considered along three distinct axes:

- *Content* – what the sign says;
- *Form* – how legible the sign is; and,
- *Location* – whether the sign is noticeable and readable before one enters the surveilled area.

### *Content*

A minimally compliant sign should contain the following items:

1. The fact that video surveillance is being conducted in the vicinity.
2. Whether images are being monitored live, or recorded, or both.
3. The name of the organization responsible for the video surveillance scheme.
4. The title and contact information for the person in the organization who is responsible for personal information protection. This should include a phone

- number for a timely response to immediate queries, as well as usual contact details for correspondence (mailing address, email contact, privacy policy URL).
5. The title of the specific privacy or personal information protection legislation that governs the handling of personal information in this situation.
  6. Contact information for the office of the relevant privacy commissioner.

### *Form*

The text of a compliant sign must be clear and visible from a reasonable distance, and the sign itself must be noticeable to the average passer-by, either through size, colour, or other means of drawing attention. In particular, the fact that there is video surveillance should be eye catching and noticeable to normally sighted people from a distance of at least 4 meters. This can be conveyed by a combination of familiar/standard graphic icons and basic text of sufficient size.

The full required contents of the sign should be normally readable at a distance of 2 meters.

Clearly defined high contrast graphic and text elements should be used, such as are conventional in highway and other safety signage norms.

A sample template for signs compliant with the Content and Form requirements can be found at [http://surveillancerights.ca/resources\\_compliance\\_details\\_web.html](http://surveillancerights.ca/resources_compliance_details_web.html)

### *Location*

Any signage to be compliant must be positioned so that it may be normally noticed and read by individuals prior to entering an area under surveillance, in order that they may avoid the cameras if they so wish. This means sign must be encountered initially in an area **not subject** to video surveillance, including at all usual entrances to the area under surveillance. Signs should be placed reasonably close to eye level and oriented so as to be readily noticeable by anyone about to enter the surveilled space. For extensive or indeterminately bounded spaces, additional signs should be posted throughout to remind people that they are still under surveillance.

### **Other compliance criteria:**

While appropriate signage is a core criterion for compliance, there are a number of other requirements spelled out in the **10 things to do when considering, planning and using video surveillance** section of *Guidelines*. These are:

1. Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.
2. Establish the business reason for conducting video surveillance and use video surveillance only for that reason.
3. Develop a policy on the use of video surveillance.
4. Limit the use and viewing range of cameras as much as possible.

5. Inform the public that video surveillance is taking place.
6. Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.
7. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.
8. Give individuals access to information about themselves. This includes video images.
9. Educate camera operators on the obligation to protect the privacy of individuals.
10. Periodically evaluate the need for video surveillance.

For the purposes of the reward, a readily available policy statement (e.g. posted on the organization's website) that documents compliance with these various *Guideline* items would suffice. In particular, such a statement should at least specify and explain the following:

- rationale(s) for video surveillance
- appropriate limitations of camera viewing range
- signage and other public information
- procedures and retention schedule for the secure storage and deletion of images
- procedures for handling queries and individual image access requests
- education program for camera operators and customer contact personnel
- periodic re-evaluation of the need for surveillance and specific aspects of implementation

## Notes

---

<sup>i</sup> Surveillance Rights website: <http://surveillancerights.ca>

<sup>ii</sup> “Guidelines for Overt Video Surveillance in the Private Sector”, March 2008, [http://www.priv.gc.ca/information/guide/2008/gl\\_vs\\_080306\\_e.cfm](http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.cfm).

<sup>iii</sup> The main pieces of Canadian legislation governing video surveillance privacy for commercial activities, and the offices of the corresponding privacy commissioners are:

Alberta: *Personal Information Protection Act*, S.A. 2003, c. P-65, administered by the Office of the Information and Privacy Commissioner of Alberta <http://oipc.ab.ca>

---

British Columbia: *Personal Information Protection Act*, S.B.C. 2003, c. 63, , administered by the Office of the Information and Privacy Commissioner for British Columbia <http://oipc.bc.ca>

Quebec: *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. , c. P-39.1, administered by the Commission d'accès à l'information <http://www.cai.gouv.qc.ca>

Other provinces and federally regulated industries: *Personal Information Protection & Electronic Documents Act*, S.C. 2000, c. 5, administered by the Office of the Privacy Commissioner for Canada <http://www.priv.gc.ca>

(See [http://www.priv.gc.ca/leg\\_c/legislation/ss\\_index\\_e.asp](http://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp) for details and updates)

For governmental bodies, the relevant public sector legislation at the federal, provincial/territorial and municipal levels applies. eg for the Government of Canada, it is the *Privacy Act* 1980-81-82-83, c. 111.