IPC

Practices

NUMBER 10
REVISED SEPTEMBER 1998

PUTTING ONTARIO'S INFORMATION AND PRIVACY LEGISLATION TO WORK
INFORMATION AND PRIVACY COMMISSIONER/ONTARIO
ANN CAVOUKIAN, Ph.D., COMMISSIONER

Video Surveillance: The Privacy Implications

Video surveillance has a high potential for infringing upon an individual's right to privacy. Institutions should therefore weigh all factors carefully to determine whether its use is appropriate.

The use of video cameras for surveillance purposes occurs in the private and public sectors. Video cameras and monitors may be encountered in places such as retail stores, financial institutions, parking lots, public transit facilities, public highways, and in the workplace (where security is an issue). Video cameras can be used to capture images of the public, office staff, or both.

After careful consideration, an institution may decide to use video surveillance for a variety of reasons. Under special circumstances, a government organization might utilize it for the purposes of theft control and overall security — for instance, to help to ensure the safety of staff working late at night. Another, more questionable use of video surveillance may be for monitoring the performance of staff — for example, in an attempt to measure their productivity.

Institutions accustomed to storing information on paper, microfilm, or computer disk need to be aware that videotapes are a vastly different medium. The kinds of images that may be captured by a video camera — such as a person's physical characteristics, voice, speech, and mannerisms — are unique and highly personal.

The general public is becoming increasingly concerned about the use of video surveillance for the collection of personal information. The Information and Privacy Commissioner/Ontario (IPC) has received privacy complaints about the use of video surveillance. In those instances, the IPC investigated whether the collection, retention, use, and disclosure of the video-recorded information was in accordance with the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*).

The IPC cautions any institution using or considering the use of video surveillance to ensure that adequate measures have been taken to comply with the privacy provisions of the *Acts*.

Covert Surveillance

The IPC is particularly concerned about covert surveillance. Covert surveillance has been defined as "the secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals, which is then recorded in material form, including notes and photographs." [From a series of guidelines produced in 1992 by the Privacy Commissioner, Australia.]

The *Acts* require that individuals be notified when their personal information is being collected regarding the purpose of the collection and the intended use(s). Covert surveillance — whether it involves the use of video equipment or other recording devices — is likely to violate an individual's right to privacy, and an institution must ask itself whether there are sufficient public interest reasons to justify its use.

Definitions

Institutions using or considering the use of video surveillance should refer to the appropriate definition section of the *Acts*.

Section 2(1) of the *Acts* includes "videotapes" in its definition of the term "record."

Section 2(1) also provides a definition of "personal information," which it describes as recorded information about an *identifiable individual*, including information relating to race, ethnic origin, colour, age, and sex. If a videotape displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under the *Acts*.

Privacy Considerations

The IPC strongly recommends that institutions answer the following important questions before determining whether the use of video surveillance is appropriate:

1. Does the information being considered for collection constitute "personal information" as defined in section 2(1) of the *Acts*?

2. Has the authority to collect the personal information been determined? If so, is there a compelling need to collect the information through the use of video surveillance? Has another manner of collection that may prove less privacy intrusive been considered?

3. Have any applicable collective agreements been reviewed to determine if it is permissible to videotape employees?

4. Has consideration been given to whether an individual might request access to his or her video information under the *Acts*? Will it be possible to "sever" the personal identifiers of any other individuals?

5. Has the *Canadian Charter of Rights and Freedoms* been referred to, particularly section 8, which provides that everyone has the right to be secure against unreasonable search or seizure?

6. Has the advice of legal counsel been sought, or has a Policy Adviser at the Corporate Freedom of Information and Privacy Office, Management Board Secretariat been consulted?

7. Has consideration been given to the *notice* provisions of the *Acts*? It is important to remember that, unless notice has been waived by the responsible Minister, individuals must be given notice of the legal authority for the collection, advised of the intended purpose(s) and put in touch with a public official who can answer questions about the collection.

Here are the specific notice provisions:

- Notice must be provided unless one of the waiver of notice clauses applies. Refer to sections 39(2) and (3) of the provincial *Act* and section 29(3) of the municipal *Act*. (For more information, read *IPC Practices*, Number 8: "Providing Notice of Collection.")

- Where collection is deemed appropriate, notification of the legal authority and purpose for the intended use of the personal information must be provided. Notice may be oral or written. The institution may consider providing notice as a sign, posted in prominent view.

- You must provide the name, business address, and telephone number of a person at your institution who can answer any questions about the collection.

8. Have your security arrangements for the retention of tape-recorded information been evaluated? It is vital that any videotape containing personal information is kept confidential and accessible only to those who need to see it in the performance of their duties. It is also important that government organizations identify each recorded tape by numbering and dating them by camera location. The individual responsible for camera operations should ensure that every time someone is given access to a tape, this is recorded in a log. This will serve as a control and an audit trail of access to the videotapes.

9. Have the use and retention provisions of the *Acts* been examined? It is important to remember that if a videotape is to be used — i.e., viewed, reviewed, etc. — it must be retained for at least one year after use,* unless the individual to whom the information relates consents to its earlier disposal.

10. Have you considered the circumstances of when video cameras should be used? Consideration should be given to recognizing the nature of incidents of crime and to restricting the use of video surveillance to periods identified as being those when there is a higher likelihood of crime occurring.

11. Will camera operations be audited? It is important that government organizations consider establishing ways to audit video camera operations. This will help ensure that only pertinent information is collected and that cameras are not used for any other purpose than was originally intended. In addition, by establishing an audit mechanism on the camera operation, institutions are better able to determine if it is feasible or necessary to continue with the video camera operation.

* *Municipal institutions please note: section 5 of Regulation 823 sets out that the retention period is to be the shorter of one year after use, or the period set out in a bylaw or resolution. Also, please refer to the IPC paper entitled: "Safe and Secure Disposal Procedures for Municipalities."*

IPC
Practices

is published regularly by the **Office of the Information and Privacy Commissioner**.

If you have any comments regarding this publication, wish to advise of a change of address or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
Telephone: (416) 326-3333 • 1-800-387-0073
Facsimile: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
Web site: http://www.ipc.on.ca

20% recycled paper, including 20% post-consumer fibre

ISSN 1188-7206