Office of the Access to Information and Privacy Commissioner
New Brunswick

Commissariat à l'accès à l'information et à la protection de la vie privée
Nouveau-Brunswick

BEST PRACTICE

Video Surveillance

Right to Information and Protection of Privacy Act and
Personal Health Information Privacy and Access Act

April 2014

Best Practices are issued to promote a better understanding of the rules of the Acts and to guide those who have to apply them.

This Best practice provides the established principles when considering video surveillance, along with a useful checklist to be used.

PROPER USE OF VIDEO SURVEILLANCE

Video surveillance should be limited to specific purposes to ensure the safety of the public and, on occasion, enforce the law. Even though these are the permitted uses, video surveillance should supplement less intrusive forms of surveillance and only be used when other types of surveillance have been deemed ineffective.

While an effective tool to ensure the safety of the public and to enforce the law, video surveillance can be exploited in an unauthorized manner and in that regard, video surveillance should NEVER be used to:

- View inside private dwellings that are not part of the surveillance;
- Look at areas of greater privacy such as washrooms or changing areas;
- Capture images of citizens not targeted by the stated purpose of surveillance; or
- For purposes of observation (i.e. spying).

OPENNESS AND TRANSPARENCY

One component to operating a compliant surveillance system is openness and transparency. Being open about the purpose of the cameras from the outset will make it easier to address any concerns of the public. Should these concerns arise, adjusting the surveillance will be less of a strain on the organization. Many of these concerns can be addressed by consulting with the public before installing the cameras. In addition, it will be important to continuously inform the public about any changes that are made to the surveillance system.

As with the installation of any video surveillance, mounting cameras in troubled areas should not be a covert operation. Posting signs in the areas under surveillance to keep individuals informed will proactively answer many of the public's questions. The presence of cameras will also dissuade individuals from committing acts that could endanger public safety or be against the law.

RETENTION, STORAGE AND SECURE DESTRUCTION

The collection of personal information in any form is subject to both pieces of legislation. This places responsibilities on public bodies and custodians to protection the personal information in their custody. Also, individuals have the right to access that information as it is considered their own personal information. As a result, it is important to ensure a proper retention, storage and secure destruction policy is in place. This policy would include timelines for how long personal information is kept and how it would be securely destroyed.

If the video footage is kept for any length of time, the recording devices should be kept in a locked or controlled-access area. A log should be kept to record all individuals who enter and exit the area of the recordings in the event there is a privacy breach.

SECURITY

As with any collection of personal information, the proper safeguards must be in place to protect the information. These information practices and security arrangements must be made clear to individuals as failure to protect the information can lead to privacy breaches.

A method of reducing the possibility that a privacy breach occurs while using video surveillance is to ensure that all video feeds are encrypted. By encrypting video feeds, there is less of a risk that unauthorized users could access the information. When a video feed is not encrypted, it is possible to purposefully (or even accidentally) intercept the signal with a wireless device.

Other steps to providing proper security of a video surveillance system would be to:

- Designate only a limited number of individuals with the responsibility for the maintenance and operation of the system;
- Properly educating the designated individuals on the purpose of, and the manner in which to use the system; and
- Take precautions that the cameras cannot be adjusted to view areas other than those that have been designated for surveillance.

In order to ensure the obligations outlined in this Best Practice are followed in the creation of a video surveillance system, please find the attached "Checklist for Video Surveillance".

<u>If you require more information about the above, please contact us at:</u>

65 Regent—Suite/Pièce 230
Fredericton, NB E3B 7H8

☎ 506.453.5965
Toll-free/Sans frais: 1.877.755.2811
🖷 506.453.5963

access.info.privacy@gnb.ca accès.info.vieprivée@gnb.ca

www.info-priv-nb.ca

CHECKLIST FOR VIDEO SURVEILLANCE SYSTEM

PROPER USES

- ☐ The video surveillance system is to ensure the safety of the public or enforce the law
- ☐ The video surveillance system supplements less intrusive forms of surveillance
- ☐ The cameras do not view inside private dwellings
- ☐ The cameras are only pointed at public areas
- ☐ The surveillance does not capture images of citizens who are not targeted by the stated purpose
- ☐ The surveillance system is not used for observation purposes

OPENNESS AND TRANSPARENCY

- ☐ The public have been advised of the purpose for the surveillance
- ☐ A public consultation has taken place
- ☐ If any changes arise in the future with the system, there is a plan in place to inform the public
- ☐ Signs have been posted to indicate the locations of the surveillance cameras
- ☐ The cameras cannot be manipulated or adjusted by unauthorized users

SECURITY

- ☐ Surveillance footage (recorded information) remains protected at all times
- ☐ Video feeds are encrypted to reduce the risk of unauthorized access
- ☐ Only authorized employees (in limited number) have access to the recorded information
- ☐ Strong and clear policies are in place regarding the protection of the collected information
- ☐ Staff have been made aware and of the requirement of compliance of all policies
- ☐ Annual audits are scheduled and conducted to ensure the security of the system and its efficiency

STORAGE AND RETENTION

- ☐ The surveillance footage is securely stored in a locked or controlled-access area
- ☐ A policy is in effect regarding the retention, storage and secure destruction of the recorded surveillance
- ☐ Logs record which employees have accessed the surveillance footage