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

GUIDE

For the use of Body-Worn Cameras by Law Enforcement

Right to Information and Protection of Privacy Act
February 2015

INTRODUCTION

BWCs technology represents a significant increase in sophistication from surveillance cameras that are set-up in a specific location, i.e. CCTV systems (please note that our Office has developed a **Best Practice** regarding Video Surveillance and a copy is available on our website www.info-priv-nb.ca or upon request).

It is understandable that law enforcement officials take advantage of new technologies to support them in their duties to protect the public. At the same time, however, technologies such as the BWCs pose serious implications for the public's right to privacy.

The intent of this Guide is to identify the privacy considerations that law enforcement authorities should take into account when deciding whether or not to outfit their officers with body-worn cameras (BWCs).

Addressing privacy considerations at the outset can allow an appropriate balance to be achieved between the needs of law enforcement and the privacy rights of individuals. This Guide is developed to be a helpful resource in that regard.

BODY-WORN CAMERAS (BWCs) CAPTURE PERSONAL INFORMATION

BWCs are recording devices designed to be worn on the uniform, glasses or helmet of a law enforcement officer, and BWCs capture:

- An audio-visual recording of events from the officer's point of view as he or she goes about the daily duties;
- High-resolution digital images that allow for a clear view of individuals and their identification; and,
- Recorded images suited to video analytics software, such as facial recognition.

In addition to images and sound, BWCs also generate metadata. Metadata is information about information, such as information about the user, the device used, and the activities taking place. Metadata may include date, time and location of the recorded activities, and when combined with that of an identifiable individual, is considered to be personal information.

BWCs therefore record personal information, or in other words, they record information "about an identifiable individual". This information is subject to the ***Right to Information and Protection of Privacy Act*** for both privacy and access to information considerations:

- The public's right to the protection of their personal information found in records held by public bodies, including provincial law enforcement authorities; and,
- The public's right to request access to recorded information held by public bodies.

As such, before implementing a BWCs program, law enforcement authorities should evaluate these considerations as well as weigh the anticipated benefits of adopting this technology against the resulting privacy intrusions and record keeping requirements.

A good question to ask is:

> ***Is it appropriate to equip law enforcement officers with cameras given the privacy implications and other considerations they raise?***

FACTORS TO CONSIDER

This Guide provides three useful factors to assist in answering that question when considering whether BWCs can be justified and necessary in your workplace or community:

Is there a specific and demonstrable need that BWCs are meant to address in your work?

What operational need has prompted you to consider BWCs as a solution?

2. Effectiveness of use of BWCs and Alternatives

Are BWCs likely to be an effective solution to your operational needs?

Has another solution been considered that may be less intrusive?

3. Benefits and Costs Analysis

Will the privacy intrusion that results from the use of BWCs be offset by significant and tangible benefits?

Would you consider first conducting a pilot project to evaluate whether BWCs deliver the required results in your community, and before fully committing to the costs and concerns that come with full implementation?

OPENNESS AND TRANSPARENCY

Perhaps the most important facet of the BWCs program remains the duty to inform the public that officers are equipped with BWCs and that people's actions and words may be recorded.

Without such transparency, there can be no "buy-in" from the public and challenges to the use of BWCs could be more common. This could render the effectiveness of BWCs less certain.

Public awareness

You can raise public awareness of the use of BWCs through the local media, social media campaigns, and on law enforcement websites. Information should include in what cases BWCs are used, for what purpose, under what authority, and who the public can contact to answer questions.

This notification is also important when law enforcement officers encounter the public and for that reason, BWCs should only be used by uniformed officers to avoid confusion.

Practical tips

While BWCs are visible on an officer's uniform or glasses, the BWCs may not be noticed by individuals particularly in stressful situations. Also, individuals may not be aware or realize that sounds are being recorded, in addition to images. Officers should therefore notify people of recording whenever possible, including that they are recording sound.

A short statement such as "**Everything you say and do is being recorded**" could be sufficient. Also, a prominent pin or sticker on the officer's uniform may be another useful option.

BEST USE OF BWCs: *TRAINING*

Given the issues surrounding the intrusion into the lives of citizens, and given that in some cases, the intrusion may be lawfully justified whereas in other cases, it may not, individuals should not be monitored by law enforcement as they go about their daily activities in public and where they are not breaking the law.

The criteria for activating BWCs should address the need to minimize, to the extent possible, the recording of innocent bystanders or innocuous interactions with the public. Admittedly, it is not possible to completely eliminate capturing images and audio of bystanders and other non-targeted individuals.

For this reason, training to law enforcement officers on the best use of BWCs and on privacy considerations should be an essential component of your BWCs program.

PROPER STORAGE, RETENTION and DESTRUCTION OF THE BWCs RECORDINGS

Because of the privacy considerations mentioned above, and the public's right of access afforded under the *Right to Information and Protection of Privacy Act*, law enforcement authorities should protect the recordings of BWCs to avoid unauthorized access or use or alterations, copying, theft or loss, as well as having a sound and secure records keeping system.

We suggest these reasonable steps be taken in that regard:

- Encrypt recordings of BWCs
- Store the recordings on a secure server
- Store hard copies of recordings in a secure storage area
    - Limit access to recordings - to those who 'need to know' their contents to do their work
- Ensure that the recordings (both video and audio) cannot be edited
    - Add an audit function to monitor inappropriate access or modifications
- Have and maintain a retention schedule (consistent with applicable laws such as *Canada Evidence Act,* police services legislation, etc.)
    - Ensure that recordings are retained for a sufficient period to afford individuals a reasonable opportunity to access their own personal information
- Have and follow a secure destruction practice of recordings at end of their retention period
- Assign specific personnel to monitor all established practices for the security of BWCs recordings (including use, access, storage and secure destruction)

ESTABLISH SOUND BWC PROCEDURES IN ONE DOCUMENT - FOR EVERYONE'S USE AND REFERENCE -

As part of any BWC program, law enforcement authorities should establish written procedures that clearly identify the reasons for implementing the BWCs in their community as well as to set out the rules of the road. The rules and procedures should be set out in one document for all your personnel's use and benefit.

The procedures document should cover the following items:

Training on use

- Roles and responsibilities of staff with regard to BWCs and their recordings
- Criteria for turning BWCs on and off
- Training to ensure that officers understand the privacy implications of BWCs and to make them aware of their responsibilities
    - Establishing consequences of not respecting these procedures
- Setting out clearly the circumstances under which recordings can be viewed and by whom
    - On a need to know basis to conduct one's work
    - Where there is reasonable grounds to view recordings
        - If not, should not be permitted to be viewed
- The purposes for which BWC recordings can be used (for ex: as evidence)
    - If training is contemplated, should establish that use of BWCs recordings is limited to minimize impact on privacy (such as blurring of faces, identifying marks, etc.)

Rules for release

- Determining the circumstances under which BWC recordings can be released to the public, if any, and the parameters in which that can take place
- Setting clear rules for those instances in which recordings can be shared outside the organization
    - For ex: with government agencies during an active investigation, or with legal representatives as part of the court discovery process, etc.

Security safeguards

- Implementing all security safeguards to ensure that recordings are kept safe, secure and integral (not inappropriately accessed or altered)
- Lay out a process to conduct regular internal audits of the BWC program to monitor and address compliance to the rules
- Establish a vetting process so that any contracts between law enforcement authorities and external service providers specify that BWCs recordings remain in the control of the authorities and are subject to applicable privacy laws

Retention and secure destruction

- Having and maintaining a retention period and secure destruction methods
    - To permit a process for access to one's personal information
    - How to securely destroy the recordings

Process in the event of a breach

- Establishing a quick response mechanism for dealing with a breach of privacy due to the unlawful access, use, copying, or disclosure of BWC recordings

Transparency and Accountability

- Public awareness campaign undertaken
    - And how and when will be continued
    - Can also contain outcomes from community consultation
        - The public's input and concerns
- Having a process where people can complain if they believe there was an unreasonable intrusion of privacy due to the use of BWCs
    - Name and contact information of staff member who can answer questions

The procedures document should be made available to the public to promote transparency and accountability. Doing so will demonstrate to the public that law enforcement authorities have set out rules and procedures to ensure the best use of BWCs, and this will go a long way to demonstrate that citizens' privacy is important, that privacy will be adequately protected, and that their right of access is being respected.

CONCLUSION

BWCs record not only actions and words of individuals, but also their association with others in the community within recording range, including friends and family. Sometimes, BWCs will record individuals in their own home.

The *Right to Information and Protection of Privacy Act* exists to protect privacy and grant to individuals the right to access their own personal information found in records held by provincial law enforcement authorities. These authorities must therefore be aware that BWCs can impact both these rights.

It is therefore prudent for law enforcement authorities to consider their operational needs while remaining mindful of these statutory rights of individuals, and to seek an appropriate balance when deciding to implement a BWC program in their community.

A procedures document will demonstrate to the public that law enforcement authorities have set out rules and procedures to ensure the best use of BWCs and demonstrate that citizens' privacy will be adequately protected and their right of access will be respected.

If you require more information about the above, please contact us at:

230- 65 Regent Fredericton, NB E3B 7H8
506.453.5965 or Toll-free 1.877.755.2811

access.info.privacy@gnb.ca

www.info-priv-nb.ca