TRANSIT POLICE

DIGITAL VIDEO SURVEILLANCE AND RECORDING SYSTEMS IN POLICE BUILDINGS

Effective Date: April 22, 2016
Revised Date:
Reviewed Date:
Review Frequency: Two Years
Office of Primary Responsibility: Privacy Officer
Office of Collateral Interest: Manager Risk and Information

POLICY

Definitions

BCPPS – British Columbia Provincial Policing Standards, as amended from time to time.

Detained person – Any person held or confined in the custody of police.

Fingerprint rooms – Any room in a police building used to fingerprint a person unless the room is used exclusively for volunteer fingerprinting.

FIPPA – British Columbia *Freedom of Information and Protection of Privacy Act,* as amended from time to time.

Interview rooms – Locations or rooms in police buildings, inside and external to a cell block, used to conduct all investigative and patrol interviews, including: “hard” and “soft” interview rooms; polygraph rooms used for detained persons; and statement and bail hearing rooms.

IT Section – The Transit Police Information Technology Section.

JPD – Jurisdictional Police Department.

Member – Designated Constable, the Chief Officer or a Deputy Chief Officer of the Transit Police.

OIPC – Office of the Information and Privacy Commissioner.

Personal Information – *FIPPA* defines “personal information” as recorded information about an identifiable individual, other than contact information. Video and audio recordings of an individual’s image and voice are included within identifiable information.

Police Act – British Columbia *Police Act*, as amended from time to time.

Privacy Officer – “Privacy Officer” as defined in *FIPPA* and as designated in writing by the Chief Officer.

Sally port – A secure parking bay immediately adjacent to a police building where detained persons are loaded or unloaded into and out of vehicles.

Transit Police – The South Coast British Columbia Transportation Authority Police Service.

Authority

1. The Transit Police is subject to and must be compliant with *FIPPA. FIPPA* provides the Transit Police authority to collect personal information for law enforcement purposes. The Transit Police is committed to ensuring the protection of individual privacy through responsible personal information management practices, including with respect to the use of video surveillance technology within police facilities. Video and audio recordings of an individual's image and voice are included as identifiable personal information.

2. The Transit Police is subject to and must be compliant with the *Police Act*, the BCPPS and the law*,* including with respect to BCPPS 4.1.1 and digital video surveillance and recordings of detained persons, victims and witnesses in police buildings.

   Note: The intent of the BCPPS is: to increase the safety of officers and the public; provide evidence for any investigation; and contribute to the consistent application of digital video surveillance and recording technology throughout the province. The principle behind these standards is to ensure that digital video surveillance and recording system is present in all interview rooms and areas of police buildings where detained persons, victims, witnesses or other persons of interest routinely interact with police agency personnel.

General

3. Transit Police personnel and contractors will be required to review and apply this policy in performing their duties and functions related to operation of the digital video surveillance and recording system with respect to Transit Police handling of detainees, witnesses and victims within an investigation.

4. The Chief Officer will be accountable for Transit Police compliance with BCPPS 4.1.1, in addition to *FIPPA,* as the Head of the Public Body.

5. Unless otherwise delegated by the Chief Officer, the Deputy Chief Officer Support Services will be responsible for day-to-day administration, oversight, audit and the Transit Police compliance with: BCPPS regarding video surveillance and recordings in police buildings; privacy obligations under *FIPPA*; and this policy.

6. As a TransLink subsidiary, the Transit Police is also required to comply with the TransLink Enterprise Video Surveillance Privacy Policy, except in relation to covert policing and counter-terrorism intelligence operations, and as otherwise permitted by Transit Police policy and the BCPPS, *FIPPA* and the law.

7. As a Designated Policing Unit in British Columbia, the Transit Police has entered into agreements with JPDs regarding operational access to police facilities and

services, including but not limited to: prisoner booking and bail hearings at detention facilities, fingerprinting, and breathalyzer test apparatus (BTA). Where JPD facilities and services are being utilized by the Transit Police, the JPD retains responsibility for compliance of their facilities and services with the BCPPS 4.1.1.

8. In the event that Members are using a JPD interview room to interview a detainee, victim or witness, the Members will be required to conduct the interview in accordance with Transit Police policies and procedures (where the comparable infrastructure is in place at the JPD interview room).

9. The Member assuming the lead investigator role will be responsible for the management/processing (i.e., collection, securing, processing and submission) of all evidence, including interview recordings and the recording of a detainee within the Transit Police facility (or other police facility if being used for an interview).

New or Modified Digital Video Surveillance Systems or Program

10. If the Transit Police plans to create a new digital video surveillance system or program, or significantly modify one, a formal *FIPPA* Privacy Impact Assessment is to be undertaken and may be submitted to the OIPC prior to implementing the proposed changes.

PROCEDURES

Digital Video Surveillance Equipment and Specifications

11. Unless exemptions are granted to the Transit Police, the Transit Police will ensure that it has digital video surveillance and recording system installed in all locations specified in the BCPPS 4.1.1, if such location is present within Transit Police operations and facilities:
    a. Sally port;
    b. Outside locations that may be used of unloading or for release of detained persons;
    c. Prisoner booking areas;
    d. Hallways and elevators inside cell block;
    e. Cells and holding/observation rooms;
    f. Interview rooms;
    g. Fingerprint rooms;
    h. Breathalyzer test apparatus rooms or areas.

12. Presently, the Transit Police does not maintain the following identified locations under BCPPS 4.1.1: detention facility (including cells, sally port, detention facility hallways, or prisoner booking area), fingerprint rooms, and breathalyzer test apparatus rooms.

13. The digital video surveillance and recording systems in each applicable location to the Transit Police will operate at a sufficient rate of speed so that recorded movement of all persons appears fluid, and enables a time and date stamp on originals recordings and any copies or extracts that are made [BCPPS 4.1.1(1)].

Operation of Digital Video Surveillance and Recording System

14. The Transit Police will require that the digital video surveillance and recording system is continuously operated when a detained person is in/at any of the locations applicable to the Transit Police [BCPPS 4.1.1(3)].

15. The Transit Police will ensure that, to the maximum extent possible, all interaction with or between detained persons while inside police buildings is restricted to areas under surveillance [BCPPS 4.1.1(4)]. [redacted]

16. The Transit Police will comply with the OIPC guidelines regarding privacy and the monitoring of persons, as well as access, security, and retention of recordings [BCPPS 4.1.1(5)].

17. [redacted]

18. [redacted]

19. [redacted]

20. [redacted]

Use of Interview Rooms

21. [redacted]

22. The Transit Police will post outside of interview rooms, signage advising individuals that they will be recorded upon entry into the room [BCPPS 4.1.1(7)]. (This is in addition to posting of signage elsewhere in the police facilities where any monitoring by video occurs.)

23. [redacted]

24. [redacted]

Solicitor-Client Privilege

25. Members will make every effort to ensure privacy and confidentiality of solicitor client privilege. To meet requirements of BCPPS 4.1.1(6), when a detained person, victim or witness requests legal consultation, Members will:

[redacted]

Victim or Witness Interview Recordings

26. To meet requirements of BCPPS 4.1.1(8), when a victim or witness requests that the interview not be recorded, Members will:

    1. Make a record of the request and time that the recording system was turned off;

    2. Have the individual sign a declaration of refusal/waiver documenting the request on the prescribed Transit Police form; and

    3. Have the other Member enter the interview room as a verifier of the proceedings to follow, in addition for security purposes.

27. If the status of the victim or witness changes during the interview process, the Member will promptly inform the individual (and restart the recording system if previously turned off pursuant to s. 26 of this policy). The Member will then inform the individual of their rights and provide the applicable police warnings, and proceed with the interview.

Securing Recordings of Incidents

28. If an incident occurs that may relate to an interview or movement of a detained person, witness or victim in a location referred to in BCPPS 4.1.1(1), Members will promptly inform their Supervisor and request that the video recordings for cameras in the location be secured for potential investigative or legal requirements. (As specified in s. 41, video recordings will then be retained for a minimum of thirteen months.)

29. If the recorded information reveals an incident that contains personal information about an individual, and the Transit Police will be using this information to make a decision that directly affects the individual, the Transit Police will retain the specified

recorded information for thirteen months after the decision is made, or as otherwise is required for lawful purpose.

Movement of Detained Persons in Police Facilities

30. [redacted]

31. [redacted]

[redacted]

[redacted]

[redacted]

Request to Access Recorded Personal Information

32. If an individual who is the subject of surveillance requests access to their recorded personal information under s. 5 of *FIPPA*, the request will be referred to the Privacy Officer or delegate for processing. However, if a victim or witness requests a copy of the interview recording at the conclusion of a police interview, or if it is in the interest of the investigation to so provide, the Member will make a copy of the recorded interview on appropriate media (e.g., DVD) and promptly provide to the requesting individual.

    1. If a copy of the interview recording is requested immediately following the interview, the Member will inform the requesting individual that the material will be provided in the language in which the interview was conducted and that there cannot be any expectation of immediate translation of transcription.

33. If an access request under s. 5 of *FIPPA* is received, the Transit Police will comply with applicable *FIPPA* requirements to withhold personal information about other individuals, including blurring or otherwise obfuscating the identity of other individuals on a video or audio recording before disclosing personal information about an individual.

34. Exemptions to the requirement of s. 31 would be as permitted by *FIPPA* ss. 15(1)(c), 15(1)(d) and 15(1)(f) (e.g., an undercover operator who is conducting the interview,

revealing a confidential source, or endangering life). In a circumstance where an exemption may apply, the Member will consult with their Supervisor as to appropriate action.

Maintenance of Equipment

35. The IT Section will be responsible for ensuring that:

    1. The digital video surveillance and recording equipment is in good technical working order;
    2. The applicable software is up to date and properly functioning; and
    3. The data storage is sufficient for interview recording.

36. Members will promptly report to the Watch Commander and IT Section when there are issues with good working order of a digital video surveillance and recording system.

37. Upon receipt of a Member's report above, the Watch Commander and IT Section will consult as to appropriate action needed, including: identifying any immediate steps to secure evidence and prevent use of equipment not meeting operating standards; informing other senior managers where appropriate; and other risk mitigation measures required.

38. The Watch Commander will, as soon as is practicable, inform the Inspectors of Operations and Support Services, and the Manager Risk and Information of significant maintenance/operational issues and when compliance with BCPPS standards is of issue. Any issues of serious concern should be brought to the attention of the Deputy Chief Officer Support Services.

Breaches, Compliance and Audit

39. To report a privacy breach or complaint, Members will follow procedures in TSML Policy No. 020 – Privacy Breach and Complaint Reporting Policy.

40. Transit Police personnel who are monitoring, operating, maintaining or securing the digital video surveillance and recording system are advised that their actions are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

41. Unless otherwise so determined by the Chief Officer, the Manager Risk and Information will cause reviews/audits to be conducted on the use and security of digital video surveillance and recording system, including monitors and storage devices.

    1. The reviews/audits will be conducted periodically at irregular intervals, documented and reported to the Deputy Chief Officer Support Services.

    2. Any concerns arising from the reviews/audits are to be addressed promptly and effectively.

Secure Retention and Disposal

42. The Transit Police will securely retain digital video surveillance recordings for a minimum of thirteen months to cover the timeframe for which a complaint may be filed under the *Police Act,* and as otherwise required for lawful police purposes, *FIPPA* and other legislation that may apply*.*

43. When replacement or external servicing of the video recording server/hardware is required, the IT Section will perform a 'Department of Defence' level wipe of information on the equipment, prior to transfer/disposal.

REFERENCES

British Columbia *Freedom of Information and Protection of Privacy Act* [RSBC 1996 Chapter 165], and OIPC Public Sector Surveillance Guidelines [January 2014]
British Columbia *Police Act* [RSBC 1996, Chapter 367]
Federal – *Access to Information Act* (R.S.C., 1985, c. A-1)
Federal – *Evidence Act* (R.S.C., 1985, c. C-5)
Federal – *Privacy Act* (R.S.C., 1985, c. P-21)
Federal – *Privacy Regulations* (SOR/83-508)
TransLink Enterprise Video Surveillance Privacy Policy [July 2008]