The following *draft* Minutes of the special meeting of the Toronto Police Services Board held on October 06, 2006 are subject to adoption at its next regularly scheduled meeting.

MINUTES OF THE SPECIAL MEETING of the Toronto Police Services Board held on October 06, 2006 at 8:30 AM in the Auditorium, Police Headquarters, 40 College, Toronto, Ontario

PRESENT:	**Dr. Alok Mukherjee**, Chair **Ms. Pam McConnell**, Councillor & Vice-Chair – via telephone **Mr. Hamlin Grange,** Member **The Honourable Hugh Locke, Q.C.,** Member
ABSENT:	**Ms. Judi Cohen,** Member **Mr. John Filion,** Councillor & Member **Mr. David Miller**, Mayor & Member
ALSO PRESENT:	**Mr. William Blair,** Chief of Police **Mr. Karl Druckman,** City of Toronto – Legal Services Division **Ms. Deirdre Williams,** Board Administrator

THIS IS AN EXTRACT FROM THE MINUTES OF THE SPECIAL MEETING OF THE TORONTO POLICE SERVICES BOARD HELD ON OCTOBER 06, 2006

#P316. CLOSED CIRCUIT TELEVISIONS PROJECT

The Board was in receipt of the following report, dated October 03, 2006, from William Blair, Chief of Police:

Subject: Closed Circuit Television

Recommendation:

It is recommended that:

(1) The Board enter into an agreement with the Ministry of Community Safety and Correctional Services relating to $2 million in funding for the "Closed Circuit Television (CCTV) – A View to a Safer Community" program; and

(2) The Board authorize the Chair to execute the legal agreement on behalf of the Board.

Background:

The Toronto Police Service (TPS) has researched the use of CCTV as a tool deployed in support of the Toronto Anti-Violence Intervention Strategy (TAVIS). The research focused on deployment in areas of the City of Toronto with elevated crime rates that are not responding to other means of police intervention. This research has reviewed a significant volume of reports from policing and government agencies around the world with respect to the design, deployment, operation, privacy impacts and governance of CCTV programs. The insight from this review has contributed to the creation of a proposal document entitled "Closed Circuit Television – A View to a Safer Community". This document is the basis for a contract with the Ontario Ministry of Community Safety and Correctional Services (the Ministry) to provide $ 2 million in funding for the purchase and deployment of a CCTV program which will be undertaken from September 2, 2006 – April 30, 2008 in the City of Toronto to record, deter and disrupt crime while increasing public safety.

The Toronto Police Service CCTV proposal has been developed to comply with the guidelines issued by the Ontario Information and Privacy Commissioner (IPC). In October 2001, the IPC released a document entitled 'Guidelines for Using Video Surveillance Cameras in Public Places', see Appendix A attached. That document identified several key areas that are to be addressed by an institution in deciding whether the collection of personal information by means of CCTV is lawful and justifiable as a policy choice, and if so, how privacy protective measures can be built into the program. The Toronto Police Service CCTV policy, under development at

this time, and to be presented to the Board at its October 19th meeting, will also be predicated upon the guidelines set out in the IPC document.

The word 'surveillance' is defined in the Miriam-Webster dictionary as 'close watch kept over someone or something'. By contrast, the word 'observation' is defined as 'designed for use in viewing something'. There is a distinction to be made in the purpose and intent of the TPS CCTV program. The TPS is not engaging in the close watch of persons through CCTV but in the observation of public spaces. The program is being designed to place CCTV in areas identified through crime analysis and community concern. Where a criminal incident occurs in the open space area under observation, the camera recording can be viewed to determine if that incident was recorded. Any such recording would provide investigative assistance and evidence that could lead to the apprehension and successful prosecution of the offender.

The deployment of the cameras in and of themselves may deter crime as has been suggested in research documents from the United Kingdom and other jurisdictions. This deterrence by mere presence mirrors provincially mandated Use of Force training that clearly identifies 'officer presence' as a meaningful mechanism to prevent and deter criminal behaviour. The deployment of CCTV may also lead to displacement of crime to areas immediately outside the deployment area. The TPS is aware of this and has set out in the proposal that the CCTV program will form part of a comprehensive crime management plan that will seek to deter crime and increase public safety in the identified area and control the displacement of crime to areas on the periphery.

Privacy and Charter Rights

The use of CCTV has been criticized as violating a person's rights both in terms of privacy and the rights enshrined in the Charter. With respect to the Charter, it is claimed that indiscriminate video surveillance, in the absence of cause, breaches the fundamental privacy rights of all Canadians protected by Sections 2 (d), 6, 7 and 8 of the Charter. The TPS CCTV policy will set out that deployment of the CCTV program will be in response to demonstrable cause justified through verifiable crime analysis and community concern.

Section 2(d) of the Charter states that everyone has the fundamental right to freedom of association. The personal information collected is accessible for viewing solely in relation to the investigation of a criminal incident occurring within the area of the camera. As prescribed by the IPC and currently in place at the TPS Video Services Unit is a mechanism and procedures for continuity and control of the video recordings to prevent unauthorized access. The CCTV policy to be presented to the Board will set out specific measures to safeguard against unauthorized access and use of personal information.

Section 6 of the Charter states that every citizen of Canada has the right to enter, remain in or leave Canada, the right to move to and take up residence in any province and the right to pursue a livelihood in any province. The TPS CCTV program in no way infringes on these mobility rights.

Section 7 of the Charter states that everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice. The very purpose of the TPS CCTV program is to make our communities safer for all citizens thereby enabling the lawful exercise of these Charter rights.

Section 8 of the Charter states that everyone has the right to be secure against unreasonable search and seizure. The design and operation of the TPS CCTV program will safeguard against violation of these rights. The design and installation will prevent viewing into private premises, through windows or other such areas where citizens have an expectation of privacy. In addition, the public notification in itself ensures that citizens are aware of the CCTV deployment and markings on the cameras ensure they are aware that these cameras are the property of the Toronto Police Service.

Privacy issues most often arise from inappropriate use of a CCTV program by the operator. Research shows abusive behaviours such as voyeurism, racial profiling, and unauthorized copying and distribution of the collected personal information.

The TPS CCTV program will not include scheduled unsupervised active monitoring by operators during the pilot. Procedure will be in place to govern use of the CCTV program and safeguard against potential misuse. The TPS CCTV program will use software to prevent viewing through windows and the unauthorized copying of personal information recorded by the camera. Continuity and control measures regarding the disclosure, duplication and transcription of video records are already established in TPS procedure 12-08. The TPS policy will provide specific measures to address the security of any such collected information. The TPS have trained two members of the Video Services Unit and two members of the Radio and Electronics Unit on CCTV design, installation, operation and protection of privacy.

IPC Guidelines for Policy Development

The IPC guidelines provide the TPS a foundation upon which to build our CCTV policy. The following are a list of considerations set out in the IPC guidelines for policy development and TPS responses.

1. The rationale and objectives for implementing the CCTV program.

The use of the TPS CCTV program is to be considered only after other measures of deterrence and prevention have been considered and have not produced the desired result. An assessment will be conducted of the effect on privacy and there will be ongoing public consultation. The CCTV program is deployed for the purpose of reducing crime and increasing public safety in the identified area.

2. The use of the CCTV program equipment, location of reception equipment and a determination of which personnel are authorized to operate the program.

The TPS Policy will identify roles and responsibilities within TPS with respect to the installation, retrieval of the video, access for viewing, copying and preparation for submission as

evidence in addition to existing policy. The deployment of the camera requires the submission of a detailed operational plan that addresses the criteria set out in item #1 above. Personal information recorded via CCTV retained for evidentiary purposes shall be stored at the TPS Video Services Unit. This unit provides centralized video asset management to the TPS and has in place court recognized continuity and control measures.

3. The institution's obligations with respect to the notice, access, use, disclosure, retention, security and disposal of records.

The TPS will place public notice signs on the periphery and within the areas in which CCTV has been deployed. These notices will inform the public that the area is under camera observation for a lawful purpose and will provide the position, contact phone number and address to which questions regarding the deployment can be directed. Such signs have already been developed by the City of Toronto for their video surveillance policy. The TPS will utilize the format of these signs for this CCTV initiative. The contact persons for the TPS CCTV pilot project will be the Staff Superintendents of Divisional Policing Command. The contact phone number will be 416-808-CCTV (2288). The TPS website will also provide information on the deployment of the CCTV program and contact person information.

CCTV use, access, and disclosure are already subject to governance through procedures 01-03 – Persons in Custody, 12-08 – Disclosure, Duplication and Transcription and 15-17 – In-Car Camera System (Pilot). Those procedures will be reviewed in terms of scope not only in relation to CCTV but overall governance issues.

With respect to records retention, the TPS has undertaken a review of the current Records Retention Schedule, City of Toronto By-law 689/2000, the records retention guidelines of the IPC, and the records retention established in the City of Toronto Video Surveillance Policy. The IPC recommends that personal information collected via CCTV be retained for a period no longer than 48 – 72 hours except where it has been viewed for law enforcement purposes in which case a separate retention schedule should be established. The City of Toronto requires that the records be retained no longer than 30 – 60 days unless a longer period is required as part of a criminal, safety, or security investigation or for evidentiary purposes. The City of Toronto policy is specific to cameras operated by the City at their owned or leased properties and was implemented as a way for the city to manage their risk issues. The City of Toronto policy does not apply to the Toronto Police Service. The City recognizes that prevention and enforcement of crime on public streets falls exclusively within the law enforcement mandate of the TPS.

The review of the TPS Records Retention Schedule will continue and will examine both the In-Car and Cell Camera retention requirements. As an interim measure, a retention period of 72 hours will apply to personal information recorded via CCTV but not viewed. Where the personal information is viewed in response to a criminal incident the record shall be retained for a period defined by occurrence type as set out in City of Toronto By-law 689/2000.

4. The designation of a senior staff member to be responsible for the institution's privacy obligations under the acts and its policy.

The Freedom of Information Co-Ordinator of the TPS is currently responsible for privacy obligations. The Staff Superintendents of Divisional Policing Command will be the senior officials responsible for the administration of the CCTV program.

5. A requirement that the institution will maintain control of and responsibility for the video surveillance program at all times.

This item flows into policy item # 3 above with respect to governance on the use, access, disclosure and retention of personal information collected via CCTV. This requirement will be represented in any agreements between the TPS and external service providers who may be utilized for various aspects of the design, installation or repair of the CCTV program.

The items discussed above and others will be set out in a draft policy to be brought before the Board on October 19th, 2006.

Measurements

The CCTV proposal and contract before the Board includes a number of measurements to assess impact in terms of effectiveness and community satisfaction. The terms of the contract with the Ministry require the submission of financial and evaluation reports at pre-defined dates in 2007 and 2008.

The impact of the use of CCTV by TPS will be measured as set out in the proposal. The measurements will focus on the change in number of reported incidents of crime in the identified area comparative to areas immediately outside it and the City as a whole. The evaluation will also utilize community consultation to gauge changes in public perception regarding the view of CCTV, privacy concerns, worry about crime, feelings of safety, visits or avoidance of identified areas and other measurements. These measurements will be conducted both pre and post deployment.

The analysis will look at the number of reported crimes and crime rates over the six month period pre-deployment, the 6 month period during which CCTV is deployed and the six month period following the removal of the CCTV program from the identified area. The Ministry has agreed that these measurements will be utilized to assess the impact of the TPS CCTV program.

The TPS will submit a report to the Board on a quarterly basis commencing April 30th, 2007, the deployment date contained in the contract, with respect to:

1. Ongoing Community Consultation – including dates, times and locations of meetings held, community concerns raised and number of meetings held.
2. Number of times that personal information recorded via CCTV is accessed in relation to a criminal incident.
3. Percentage of reported incidents recorded by CCTV where a person was charged.
4. Number of calls to 416-808-CCTV (2288) and a summary of the identified issues.
5. Financial details related to the CCTV contract with the Ministry
6. Issues arising from the TPS CCTV initiative that need to be resolved.

The TPS will also submit to the Board any financial and evaluation reports that the TPS is contractually obligated to submit to the Ministry with respect to this CCTV initiative.

Community Consultation

Ongoing community consultation is a key component to the success of the TPS CCTV initiative and is a requirement under the terms of the contract with the Ministry. The TPS has already met with members of Community Police Liaison Committees in 31 and 42 Division and future meetings are being planned. These meetings provide an opportunity for the TPS to engage our community partners and invite input relating to the impact of the use of CCTV. This requires engaging the broad spectrum of our diverse communities in open discussion of our policing initiatives, soliciting their opinions, comments and concerns and addressing issues raised.

The community consultation component of this CCTV initiative is in the beginning stages and will expand and be ongoing as the project moves forward. The TPS will seek to gauge community perception of crime and CCTV as a crime management tool through a survey mechanism that will provide meaningful analysis of customer satisfaction and quality of life questions. Through this consultation strategy, the TPS will be able to review this CCTV initiative in terms of its value and make a determination as to its continuance, expansion or discontinuance.

The value of CCTV to deter crime and increase public safety is an unknown entity in the City of Toronto. Citizens are repeatedly exposed to CCTV in virtually all aspects of their lives from shopping, using banking services, fueling their vehicles or traveling on highways. This CCTV project has been developed with significant consideration for the protection of privacy rights enjoyed by our citizens. This CCTV initiative, as supported by the Ministry, is proposed with a view to creating a safer community for the citizens of the City of Toronto.

Deputy Chief Kim Derry will be in attendance to respond to any questions that the Board may have.

Deputy Chief Kim Derry, Divisional Policing Command, and Staff Sergeant Mark Barkley, Communications Services, were in attendance and responded to questions by the Board about this report.

The Board noted that the foregoing report refers to the CCTV project as a "pilot". Chief Blair confirmed that the project will be operating as a pilot project in two specific areas: No.s 31 and 42 Divisions. Chief Blair also advised that he will provide a further report to the Board if the pilot project is extended beyond the two pilot locations.

The Board approved the foregoing.

Appendix "A"

Information and Privacy Commissioner/ Ontario

Guidelines for Using Video Surveillance Cameras in Public Places

Ann Cavoukian, Ph.D.
Commissioner
October 2001

Acknowledgements

These *Guidelines* build on those developed by the British Columbia Information and Privacy Commissioner's *Public Surveillance System Privacy Guidelines*, dated January 26, 2001, and the *Guide to Using Surveillance Cameras in Public Areas*, issued by the Government of Alberta's Freedom of Information and Protection of Privacy Office, dated April 2001. These sources are gratefully acknowledged.

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Judith Hoffman in preparing this report.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

1. Introduction

Government institutions are considering the implementation of video surveillance technology with increasing frequency for the purposes of general law enforcement programs and public safety programs. In limited and defined circumstances, video surveillance cameras may be appropriate to protect public safety and detect or deter criminal activity.

Institutions governed by the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) that are considering implementing a video surveillance program must balance the benefits of video surveillance to the public against an individual's right to be free of unwarranted intrusion into his or her life. Pervasive, routine and random surveillance of ordinary, lawful public activities interferes with an individual's privacy.

These *Guidelines* are intended to assist institutions in deciding whether the collection of personal information by means of a video surveillance system is lawful and justifiable as a policy choice, and if so, how privacy protective measures can be built into the system.

These *Guidelines* do not apply to surveillance when used as a *case-specific investigation tool* for law enforcement purposes where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

Covert surveillance is surveillance conducted through the use of hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of this technology is required, as set out in Appendix A.

These guidelines are also not intended to apply to workplace surveillance systems installed by an institution to conduct workplace surveillance of employees.

2. Definitions

In these *Guidelines*:

Personal information is defined in section 2 of the *Acts* as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If a video surveillance system 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*.

Record, also defined in section 2 of the *Acts*, means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

Video Surveillance System refers to a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces (including streets, highways, parks). In these *Guidelines*, the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

Reception Equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Storage Device refers to a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

3. Collection of Personal Information Using a Video Surveillance System

Any recorded data or visual, audio or other images of an identifiable individual qualifies as "personal information" under the *Acts*.

Since video surveillance systems can be operated to collect personal information about identifiable individuals, institutions must determine if they have the authority to collect this personal information in accordance with the *Acts*.

Pursuant to section 38(2) of the provincial *Act* and section 28(2) of the municipal *Act*, no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Institutions must be able to demonstrate that any proposed or existing collection of personal information by a video surveillance system is authorized under this provision of the *Acts*.

4. Considerations Prior to Using a Video Surveillance System

Before deciding to use video surveillance, it is recommended that institutions consider the following:

- A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.

  Video surveillance should only be used where conventional means (i.e., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.

- The use of **each** video surveillance camera should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.

- An assessment should be conducted of the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated. Institutions may wish to refer to the Ontario Government's Privacy Impact Assessment tool.[1]

- Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public. Extensive public consultation should take place.

- Institutions should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

[1] This document is available at <www.gov.on.ca/mbs/english/fip/pia>.

5. Developing the Policy for a Video Surveillance System

Once a decision has been made to use a video surveillance system, an institution should develop and implement a comprehensive written policy for the operation of the system. This policy should include:

- The rationale and objectives for implementing the video surveillance system.
- The use of the system's equipment, including: the location of the reception equipment; which personnel are authorized to operate the system, and the times when video surveillance will be in effect.
- The institution's obligations with respect to the notice, access, use, disclosure, retention, security and disposal of records in accordance with the *Acts*. (See Section 7.)
- The designation of a senior staff member to be responsible for the institution's privacy obligations under the *Acts* and its policy.
- A requirement that the institution will maintain control of and responsibility for the video surveillance system at all times.
- A requirement that any agreements between the institution and service providers state that the records dealt with or created while delivering a video surveillance program are under the institution's control and subject to the *Acts*.
- A requirement that employees and service providers review and comply with the policy and the *Acts* in performing their duties and functions related to the operation of the video surveillance system.

  Employees should be subject to discipline if they breach the policy or the provisions of the *Acts* or other relevant statutes. Where a service provider fails to comply with the policy or the provisions of the *Act*, it would be considered a breach of contract leading to penalties up to and including contract termination.

  Employees of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the *Acts*, including an undertaking of confidentiality.
- A requirement that there is a process in place to appropriately respond to any inadvertent disclosures of personal information.[2]

[2] See *A Privacy Breach Has Occurred – What Happens Next?* Presented by staff of the Information and Privacy Commissioner/Ontario at the Open Government 2001 – Access & Privacy Workshop. September 14, 2001. Available at <www.ipc.on.ca>.

- The incorporation of the policy into training and orientation programs of an institution and service provider. Training programs addressing staff obligations under the *Act* should be conducted on a regular basis.

- The policy should be reviewed and updated regularly, at least once every two years.

6. Designing and Installing Video Surveillance Equipment

In designing a video surveillance system and installing equipment, the institution should consider the following:

- Reception equipment such as video cameras, or audio or other devices should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity.

- The equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings.

- If cameras are adjustable by operators, this should be restricted, if possible, so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video surveillance program.

- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g., change rooms and washrooms).

- The institution should consider restricting video surveillance to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance.

- The public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance areas, of video surveillance equipment locations, so the public has reasonable and adequate warning that surveillance is or may be in operation before entering any area under video surveillance. As a minimum requirement, signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system and include an address and telephone number for contact purposes.

- In addition, notification requirements under section 39(2) of the provincial *Act* and section 29(2) of the municipal *Act* include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of someone who can answer questions about the collection. This information can be provided at the location on signage and/or by other means of public notification such as pamphlets. (Minimal requirements for signage are noted in the preceding paragraph.)

- Institutions should be as open as possible about the video surveillance program in operation and upon request, should make available to the public information on the rationale for the video surveillance program, its objectives and the policies and procedures that have been put in place. This may be done in pamphlet or leaflet form. A description of the program on an institution's website might also be an effective way of disseminating this information.

- Reception equipment should be in a strictly controlled access area. Only controlling personnel, or those properly authorized in writing by those personnel according to the institution's policy, should have access to the controlled access area and the reception equipment. Video monitors should not be in a position that enables public viewing.

7. Access, Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records

Any information obtained by way of video surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect public safety or to detect and deter criminal activity. Information should not be retained or used for any other purposes.

If the video surveillance system creates a record by recording personal information, the following policies and procedures should be implemented by the institution and should be included in the institution's policy discussed under Section 5:

- All tapes or other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area. Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol.

- Access to the storage devices should only be by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.

- The institution should develop written policies on the use and retention of recorded information that:
  - Clearly state who can view the information and under what circumstances (i.e., because an incident has been reported, or to investigate a potential crime).
  - Set out the retention period for information that has not been viewed for law enforcement or public safety purposes. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule (normally between 48 and 72 hours).
  - Establish a separate retention period when recorded information has been viewed for law enforcement or public safety purposes. If personal information is used for this purpose, section 5(1) of Ontario Regulation 460 under the provincial *Act* requires the recorded information to be retained for one year. Although section 5 of Ontario Regulation 823 under the municipal *Act* contains this provision, a resolution or by-law may reduce retention periods.

    Municipal institutions should consider passing a by-law or resolution, as contemplated by section 5 of Ontario Regulation 823, that makes their retention schedules explicit.
- The institution should store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A storage device release form should be completed before any storage device is disclosed to appropriate authorities. The form should indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use. This activity should be regularly monitored and strictly enforced.
- Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing the personal information.
- An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information under section 47 of the provincial *Act* and section 36 of the municipal *Act*. Policies and procedures must recognize this right. Access may be granted to one's own personal information in whole or in part, unless an exemption applies under section 49 of the provincial *Act* or section 38 of the municipal *Act*. Access to an individual's own personal information in these circumstances may also depend upon whether any exempt information can be reasonably severed from the record.

8. Auditing and Evaluating the Use of a Video Surveillance System

Institutions should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the institution's compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed immediately.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

The institution should regularly review and evaluate its video surveillance program to ascertain whether it is still justified in accordance with the requirements in Section 4. This evaluation should occur at least once a year.

9. Other Resources

The personal information recorded by an institution's video surveillance system, and the institution's policies and practices respecting the personal information, are subject to the privacy protection provisions of the *Acts*.

Prior to implementing a video surveillance system or, for that matter, any new program with privacy implications, institutions should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator. Management Board Secretariat's Information and Privacy Office is a useful resource for Co-ordinators.

The Information and Privacy Commissioner/Ontario monitors compliance with the privacy protection provisions of the *Acts*. If an institution intends to introduce, significantly modify or expand a video surveillance system, they should consult with the Office of the Information and Privacy Commissioner/Ontario.

Appendix A — Covert Surveillance

Covert surveillance refers to surveillance conducted by means of hidden devices and should only be used as an absolute last resort. Prior to deciding to use covert surveillance for a purpose other than a case-specific law enforcement activity, institutions should conduct a comprehensive assessment of the privacy impacts associated with the implementation of such a program. Institutions should submit this assessment, together with the case for implementing covert surveillance, to the Office of the Information and Privacy Commissioner/ Ontario. See Section 9 for additional resources.

The purpose of the assessment is to ensure that covert surveillance is the only available option under the circumstances and that the benefits derived from the personal information obtained would far outweigh the violation of privacy of the individuals observed.

A law enforcement agency that uses covert surveillance as a case-specific investigation tool for law enforcement purposes may consider developing, as part of sound privacy protection practices, a protocol that establishes how the decision to use covert surveillance is made on a case-by-case basis. The protocol could also include privacy protection practices for the operation of the system.

THIS IS AN EXTRACT FROM THE MINUTES OF THE SPECIAL MEETING OF THE TORONTO POLICE SERVICES BOARD HELD ON OCTOBER 06, 2006

#P317. ADJOURNMENT

_____

Alok Mukherjee
Chair