Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report

March 2008

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report

Introduction

The significant growth of video surveillance cameras throughout the world, especially as witnessed in the United Kingdom, has created considerable concerns with respect to privacy. This Report was prompted by a complaint received from Privacy International regarding the Canadian expansion of the use of video surveillance cameras in the City of Toronto's mass transit system. In light of the divergent points of view on video surveillance, in addition to investigating this complaint, my office decided to expand our Report to include a review of the literature, as well as an examination of the role that privacy-enhancing technologies can play in mitigating the privacy-invasive nature of video surveillance cameras. As such, this Report is longer than most, attempting to provide a comprehensive analysis examining the broader context of video surveillance. Given the enormous public support for the use of video surveillance cameras in mass transit systems and by the law enforcement community, addressing this issue broadly, with a view to seeking a positive-sum paradigm through the use of privacy-enhancing technologies, is our ultimate goal.

Background

On October 24, 2007, the Office of the Information and Privacy Commissioner of Ontario (IPC) received a letter of complaint from an organization relating to the deployment of video surveillance cameras throughout the Toronto Transit Commission's (TTC) mass transit system in Toronto, Ontario. The organization subsequently publicly identified itself as Privacy International, which is based in the United Kingdom.[1]

The letter of complaint expressed the view that the TTC's use of video surveillance cameras contravened the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). In their letter, Privacy International argued that the collection principles of the *Act* "are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers." It argued that the program has been undertaken on the basis of crime prevention and crime detection despite the fact that there is no evidence that video surveillance on public transit systems significantly reduces the level of crime or the

1 The letter of complaint has been posted to Privacy International's website: **http://www.privacyinternational.org/issues/compliance/complaint_ttc_privacy.pdf**

threat of terrorist attacks. It also argued that studies indicate that video surveillance has a marginal impact on investigations and that video surveillance cameras are plagued with technological and management issues. Finally, Privacy International stated that the TTC had failed to respect legal requirements for public consultation, disclosure and establishment of a public interest case for its video surveillance system. In order to address these issues, this privacy complaint file was opened (MC07-68), and an investigation commenced.

Before outlining the investigation of this complaint, I will first provide background information on the privacy implications of video surveillance cameras and the manner in which these issues have been addressed by my office over the years. I will also include a discussion of the research on the effectiveness of video surveillance, since this is a pivotal issue in this investigation. For those who may only be interested in the investigation itself, please proceed directly to that part of the report dealing with the specifics of the investigation, beginning on page 74.

Privacy and Video Surveillance

Historically, pervasive video surveillance has posed a threat to privacy and constitutional rights. When controlled by government departments, video surveillance can provide the government with massive amounts of personal information about the activities of law-abiding citizens, going about their daily lives. When individuals know they are being watched, this may have a chilling effect on their freedom to speak, act and associate with others. Since individuals may censor their own activities when they are aware of being watched, video surveillance may also be perceived as a means of enforcing social conformity.

Privacy and the right of individuals to go about their daily activities in an anonymous fashion not only protects freedom of expression and association, but also protects individuals from intrusions into their daily lives by the government. Accordingly, when government organizations wish to use surveillance technology in a manner that will impact the privacy of all citizens, there must be clear justification for doing so. Specifically, the benefits of the technology should justify any invasion of privacy.

It has been argued that individuals cannot have a reasonable expectation of privacy in public places, especially in the case of urban mass transit systems where large volumes of people may be concentrated in relatively restricted spaces. In addition, it has been argued that video surveillance in such places is an enhancement of a person's natural ability to observe what is happening in public. While the expectation of privacy in public spaces may be lower than in private spaces, it is not entirely eliminated. People *do* have a right to expect the following: that their personal information will only be collected for legitimate, limited and specific

purposes; that the collection of their personal information will be limited to the minimum necessary for the specified purposes; and that their personal information will only be used and disclosed for the specified purposes. These general principles should apply to all video surveillance systems.

In order to address situations where government organizations elect to deploy video surveillance systems, my office issued *Guidelines for the Use of Video Surveillance Cameras in Public Places* (the *Guidelines*), in 2001. These *Guidelines* were later updated in 2007,[2] and are based on the provisions of Ontario's *Freedom of Information and Protection of Privacy Act* and its municipal counterpart, the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*). Since they were issued, the *Guidelines* have been used by many government organizations to develop and implement video surveillance programs in a privacy-protective manner, in compliance with the *Acts*.

The *Guidelines* are intended to assist organizations in determining whether the collection of personal information by means of video surveillance is lawful and justifiable as a policy choice, and if so, how privacy-protective measures may be built into the system. The *Guidelines* do not apply to covert surveillance, or 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.

Before deciding whether to use video surveillance, the *Guidelines* recommend that organizations consider the following:

- A video surveillance system should only be adopted after other measures to protect public safety or to deter, detect, or assist in the investigation of criminal activity have been considered and rejected as unworkable. Video surveillance should only be used where conventional means (e.g., 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 video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- An assessment should be made of the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects may be mitigated.

2 These *Guidelines* are available online:
http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf

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

Once a decision has been made to deploy video surveillance, the *Guidelines* set out the manner in which video surveillance cameras should be implemented in order to minimize their impact on privacy.

I have taken these *Guidelines* into consideration in investigating the TTC's video surveillance program.

Evidence of the Effectiveness of Video Surveillance

In its letter of complaint, Privacy International made reference to empirical studies addressing the efficacy of video surveillance. Since there is considerable disparity in the views relating to its efficacy, my office decided to conduct a selective review of the literature on the effectiveness of video surveillance on potential offenders and on criminal justice processes and outcomes. The focus of the review was on research conducted over the past 10 years.

The literature review found numerous studies on the effectiveness of video surveillance on crime, in a broad range of settings. These studies varied substantially, however, in terms of their methodological rigour. Since an in-depth review of each of these studies was not feasible within the course of our investigation, we decided to rely on the work of credible experts who evaluated a broad range of studies on the topic and drew their conclusions on the basis of the quality of the empirical evidence before them.

There are significant challenges to conducting high-quality research on video surveillance in natural settings because of the difficulty of controlling the multitude of extraneous factors that may influence the research outcomes. In order to demonstrate the effectiveness of video surveillance on crime prevention, a study would have to show either a decrease in the rate of crime, or a slowing in an increasing crime rate in locations where video surveillance cameras had been implemented. To confirm that any such change was attributable to video surveillance, a study would have to show that a similar decrease in crime or a slowing in the increasing crime rate did not occur in comparable locations where video surveillance cameras had not been implemented (control areas). In addition, in order to confirm that such changes in crime rates were long-term as opposed to transient, the evaluation

period would have to extend for a substantial period of time. Unfortunately, research with this level of methodological rigour is extremely rare.

In 1997, California-based Marcus Nieto examined whether the use of video surveillance in public and private places was effective in preventing crime and concluded that the data suggested that the technology was successful in both reducing and preventing crimes, and was helpful in prosecuting individuals caught in the act of committing a crime.[3] Nieto looked at evaluations of the technology from around the world.

In 2001, in its *Final Report: Evaluation of the NSW Government Policy Statement and Guidelines for Closed Circuit Television (CCTV) in Public Places*, the Inter-departmental Committee on video surveillance reported on an evaluation of video surveillance technology throughout New South Wales, Australia.[4] The committee concluded that the anecdotal reports and statistics provided an indication that video surveillance may be effective in certain contexts and had received a high level of support. However, the committee noted that none of the assessments could be viewed as systematic evaluations of the technology.

In 2003, the Royal Canadian Mounted Police commissioned an evaluation of the effects of video surveillance systems on crime.[5] Wade Deisman, Professor of Criminology and Director of the multidisciplinary National Security Working Group at the University of Ottawa, conducted the evaluation. The review showed that "the effects of video surveillance on crime are quite variable and fairly unpredictable"[6] and that the deterrent value of video surveillance varies over time and across crime categories. Video surveillance systems were found to have the least effect on public disorder offences.[7] The magnitude of the deterring effects of video surveillance on crime was found to depend on the location, with the greatest benefit being in parking lots. The evaluation also found that video surveillance cameras did not need to be operational in order to deter crime. The deterring effects were highest when video surveillance was used in conjunction with other crime reduction measures and when tailored to the local setting. Continuing publicity was also required to maintain the positive effects of video surveillance systems on

3 See Marcus Nieto, *"Public video surveillance: is it an effective crime prevention tool?"* Sacramento: California Research Bureau, California State Library, June 1997.

4 See "*Final report: evaluation of the NSW government policy statement & guidelines for closed circuit television (CCTV) in public places,"* prepared for the Inter-Departmental Committee on CCTV c/o Crime Prevention Division, Attorney General's Department, July 2001 online: **http://www.dlg.nsw.gov.au/Files/Information/CCTV%20final%20report.PDF**

5 See Wade Deisman, *"CCTV: literature review and bibliography,"* Research and Evaluation Branch, Community, Contract and Aboriginal Policing Services Directorate, Royal Canadian Mounted Police, 2003, available online by request: **http://www.rcmp-grc.gc.ca/ccaps/cctv_e.htm**

6 *Ibid*, page 2.

7 Public disorder offences may include acts of violence and/or intimidation by individuals or groups of individuals, such as rioting and drunkenness.

crime, over time. No evidence was found of increased conviction rates with the implementation of video surveillance.

In 2002, the Home Office in the United Kingdom issued a report entitled, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*.[8] The report was written by Brandon Welsh, Professor in the Department of Criminal Justice at the University of Massachusetts Lowell, and David Farrington, Professor of Psychological Criminology in the Institute of Criminology at the University of Cambridge. The authors assessed 46 relevant studies from both the United States and Britain according to strict methodological criteria and found that only 22 studies were rigorous enough to include in their analysis. On the basis of these 22 studies, they concluded that video surveillance reduced crime to a small degree and was most effective at reducing vehicle crime in parking lots. Video surveillance was found to have little or no effect on crime in public transport and city centre settings.

In 2005, the Home Office in the United Kingdom issued another report on a study of the effectiveness of video surveillance systems.[9] Martin Gill, Professor of Criminology at the University of Leicester, directed the evaluation. The report provides a systematic evaluation of 13 video surveillance projects implemented in a range of contexts, including town centres, city centres, parking lots, hospitals and residential areas. The results were contradictory – crime went down in some target areas while it went up in others. Video surveillance systems installed in mixed category areas (e.g., parking lots, a hospital, etc.) showed the greatest reduction in crime, particularly in parking lots. Impulsive crimes, such as alcohol-related ones, were found to be less likely to be reduced than premeditated crimes, such as auto theft. Violence tended to increase while auto theft tended to decrease, in accordance with trends in national crime statistics.

It is important to note that regardless of the inconclusiveness of the empirical research on the effectiveness of video surveillance, the Home Office in the United Kingdom has not been deterred from supporting the use of this technology. A report issued in October 2007 entitled *National CCTV Strategy* stated that video surveillance plays a significant role in protecting the public and assisting the police in the investigation of crime.[10] It went on to state that the technology has been instrumental in helping the police to identify and bring to justice those involved in all

8 See Brandon C. Welsh and David P. Farrington, *"Crime prevention effects of closed circuit television: a systematic review,"* Home Office Research Study 252 online: **http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf**

9 See Martin Gill and Angela Spriggs, *"Assessing the Impact of CCTV,"* Home Office Research Study 292, February 2005 online: **http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf**

10 See Graeme Gerrard, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill and Sarah Douglas, *"National CCTV Strategy,"* Home Office, October 2007 online: **http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.pdf**

aspects of criminality, including serious crimes and terrorist incidents. The report noted that the contribution that video surveillance has made to the protection of the public and assisting the police in investigating crime has been realized despite the fact that the technology has been "developed in a piecemeal fashion with little strategic direction, control or regulation."[11] The report recommended the development of a strategy to maximize the potential of the video surveillance infrastructure.

In 2006, the United States Department of Justice, Office of Community Oriented Policing Services issued a report entitled *Video Surveillance of Public Places*.[12] The report was written by Jerry Ratcliffe, Professor in the Department of Criminal Justice at Temple University. The report provides an overview of video surveillance systems, explores the benefits and problems associated with the technology, and summarizes the findings of numerous evaluations.

The report notes that while there is a general perception among system managers and the public that video surveillance cameras are effective in preventing crime, actual evidence of crime reduction is more difficult to find. Nevertheless, based on the evidence provided by several evaluation reviews, the general findings were as follows:

- Video surveillance is more effective at reducing property crime than violent or public order crime (although there have been some successes in this area);
- Video surveillance appears to work best in small, well-defined areas (such as public parking lots);
- The individual context and the way the system is used appear to be important;
- Achieving statistically significant reductions in crime is difficult due to normal fluctuations in crime rates;
- The involvement of the police is an important determinant of the success of a system; and
- There is an investigative benefit to video surveillance once an offence has been committed.

In summary, the author concluded that, "it is possible to say there was some evidence of crime reduction in most of the systems … there is a growing list of evaluations that suggest CCTV has had some qualified successes in reducing crime." [13]

11 *Ibid*, page 5.

12 See Jerry Ratcliffe, *"Video Surveillance of Public Places,"* Problem-Oriented Guides for Police, Response Guides Series No. 4, U.S. Department of Justice, Office of Community Oriented Policing Services, 2006 online: **http://www.cops.usdoj.gov/mime/open.pdf?Item=1693**

13 *Ibid*, page 20.

Discussion of the Empirical Research on Video Surveillance

It should be noted that applications of video surveillance vary widely in many aspects. This makes it difficult to make comparisons across studies and to draw general conclusions from the evaluations. For example, applications vary in terms of the following:

- the goals of the applications;
- types of video surveillance technology used;
- passive versus active monitoring of videos;
- types of target areas (e.g., closed versus open);
- size of the target areas;
- density of cameras;
- fixed versus redeployable cameras; and
- involvement of law enforcement.

In addition, while the empirical evidence in support of the effectiveness of video surveillance in combating crime is weaker than might be expected, it is important to note that most of the research has been carried out in the United Kingdom, where video surveillance technology has proliferated, in part, due to substantial amounts of federal government funding. In contrast, the introduction of video surveillance cameras in Ontario has been more selective as it has not yet received large-scale funding from either the federal or provincial governments. Since research shows that situational factors influence the effectiveness of video surveillance cameras, the research findings from other jurisdictions, such as the United Kingdom, may not be directly applicable in the Ontario context.

For example, while video surveillance systems have shown little effect on crime in town centres and city centres in the United Kingdom, a study of the effectiveness of video surveillance cameras on crime in Sudbury, Ontario, showed very positive results.[14] Specifically, the study found that after the first camera was installed, crime rates in the downtown area dropped dramatically. It was estimated that between 300 and 500 robberies, assaults, thefts and other criminal offences have been deterred by the video surveillance project, saving as much as $800,000 in direct monetary losses. In addition, arrests relating to prostitution and drug offences increased by an average of 18 per cent per year, as a direct result of enhanced capacity to detect these crimes. The authors concluded that the video surveillance system had been effective in both deterring and detecting crime.

14 See *"Evaluation of Lion's Eye in the Sky Video Monitoring Project,"* KPMG, 2000.

The discrepancy between the findings in the United Kingdom and those in Ontario could be due to situational variations in the application of the technology. For example, one could speculate that video surveillance systems may be deployed in a more strategic manner in locations where funding for such initiatives is scarce. This may result in greater reductions in local crime rates in such locations when compared to locations where funding is more abundant.

It is also important to note that the research on the effectiveness of video surveillance has been plagued by methodological flaws, most notably the following:

- Lack of suitable control areas (i.e., areas where crime rates have not been influenced by the implementation of other crime prevention measures during the study period);
- Lack of adequate crime statistics (e.g., statistics may not be isolated to the targeted area);
- Crime rates may not be reliable indicators due to changes in the definitions of crimes and changes in the way crimes are reported over time (i.e., individuals may be less inclined to report crimes if they believe there are video surveillance cameras in the area or individuals may be more inclined to report crimes if they believe the police will be able to apprehend criminals due to the availability of video surveillance images that may be used as evidence);
- No assessment of displacement or diffusion of benefits into surrounding areas;
- Inadequate pre- and post-video surveillance time periods in which data are collected;
- The fact that video surveillance may actually increase the detection of certain types of crimes, thereby driving reported crime rates up;
- Many evaluations involved dated video surveillance technology that may be less useful for identifying offenders in comparison to the newer video surveillance technology;
- Video surveillance is seldom implemented in isolation – it is usually implemented as one component of a package of crime prevention measures and therefore its effects are difficult to isolate;
- Cameras are sometimes located in target areas with crime rates that are too low to notice a difference following the implementation of video surveillance cameras;
- Video surveillance cameras are often implemented in a piecemeal manner, making it difficult to compare crime statistics before and after implementation;

- Crime rates vary naturally over time and show evidence of seasonality and long- and short-term trends, making it difficult to isolate the effects of video surveillance cameras and making it difficult to obtain statistically significant results;
- Lack of clear objectives for implementing video surveillance cameras, making it difficult to find suitable effectiveness measures;
- Offenders may not be aware of the presence of cameras, making it virtually impossible to deter crime; and
- Very little of the research has been conducted by independent third parties.

Unfortunately, there are no clear conclusions to be drawn. There are substantial challenges in finding statistically significant evidence that video surveillance reduces crime and aids in criminal justice processes. However, it is equally difficult to conclude from the ambiguous findings reported in the literature that video surveillance is not, in fact, effective in deterring criminal activity. This conclusion is supported by other evidence on the effectiveness of video surveillance, particularly in the detection and investigation of crime, which is clearly much less equivocal than the research on the effects of video surveillance in deterring crime.

For example, in 1993, video surveillance images of toddler Jamie Bulger being led away from a Merseyside shopping mall by his two 10-year-old abductors assisted the police in identifying and apprehending his murderers.[15] Video surveillance footage released to the public led to early identification of suspects and played an important role in their subsequent prosecution in the case of the Brixton nail bomber in 1999 and in the failed bombing of London's subway system on July 21, 2005. In the later case, four men were found guilty of conspiracy for murder for their involvement.[16] More recently, images collected from video surveillance cameras located in a hospital in Sudbury, Ontario, were highly instrumental in identifying and locating a woman who pleaded guilty to having kidnapped a newborn infant from the hospital.[17] Images collected from the camera were very helpful in the return of the infant to his family.

The efficiency with which video surveillance footage has been used in the investigation of terrorism in London dramatically altered perceptions about video surveillance. For example, Nigel Brew, in a research note entitled *An Overview of the Effectiveness of Close Circuit Television (CCTV) Surveillance,* prepared for the government of

15 See the article by Shirley Lynn Scott, *"The Video Tape"* at the Crime Library website online: **http://www.crimelibrary.com/notorious_murders/young/bulger/4.html**

16 See *"4 Guilty in Failed 2005 London Bombing,"* New York Times, July 9, 2007, online: **http://www.nytimes.com/2007/07/09/world/europe/09cnd-london.html?hp**

17 See *"Woman pleads guilty to Sudbury baby abduction,"* CanWest News Service, November 24, 2007, online: **http://www.nationalpost.com/news/story.html?id=121816**

Australia in 2005, concluded that "video surveillance may be of more value as a source of evidence than as a deterrent."[18] However, as argued by Michael Greenberger, Director of the University of Maryland Centre for Health and Homeland Security, following the terrorist attacks in 2005, the "effective investigatory use of CCTV is very likely to be a significant deterrence to future terrorist activities on London mass transit."[19]

Conclusions from the Empirical Research on Video Surveillance

Since the bulk of the empirical research is deficient in a number of respects, it is difficult to draw any definitive conclusions about the effectiveness of video surveillance cameras. Without an ability to control the many factors that influence outcomes and the context and mechanisms that produce these outcomes, it is not surprising that the results of earlier evaluations have been mixed, conflicting and, at times, contradictory. Video surveillance systems do not appear to have uniform effects across a wide range of crime categories. At present, it is difficult to find unequivocal evidence that video surveillance deters or prevents crime. However, it is equally difficult to conclude the opposite. A more valuable role for video surveillance may be as a source of evidence in the detection and investigation of crime. A much larger body of research, with a consistent degree of methodological rigour, is needed before definitive statements may be made.

Why Video Surveillance Is Believed to Enhance Public Safety

Historically, video surveillance was most often implemented in public spaces because of an expectation of crime deterrence.[20] In general, the goal of deterrence and crime prevention strategies is to put in place practices or conditions that will lead potential offenders to refrain from engaging in criminal activities, delay criminal actions, or avoid a particular target. As is the case with many crime prevention strategies, video surveillance aims to make the potential offender believe that there is an increased risk of apprehension. To increase the perception of risk, the potential offender must be aware of the presence of the cameras and believe that

18 See Nigel Brew, *"An overview of the effectiveness of closed circuit television (CCTV) surveillance,"* Research Note no. 14 2005-06, Parliament of Australia, Foreign Affairs, Defense and Trade Section. October 28, 2005, page 6 online: **http://www.aph.gov.au/Library/pubs/rn/2005-06/06rn14.htm**

19 See the Abstract for Michael Greenberger, *"The need for closed circuit television in mass transit systems,"* Law Enforcement Executive Forum. 6(1), 2006 online: **http://www.umaryland.edu/healthsecurity/docs/CCTV%20in%20Mass%20Transit%20Systems.pdf**

20 See Jerry Ratcliffe, *"Video Surveillance of Public Places,"* Problem-Oriented Guides for Police, Response Guides Series No. 4, U.S. Department of Justice, Office of Community Oriented Policing Services, 2006 online: **http://www.cops.usdoj.gov/mime/open.pdf?Item=1693**

the cameras present sufficient risk of capture to outweigh the rewards of the intended crime. Awareness of the cameras may be enhanced through public education, clear signage, and media coverage of incidents caught on camera. In addition to awareness, however, understanding the consequences of being caught by the cameras requires rational thought. It is unlikely that potential offenders under the influence of drugs or alcohol would be deterred from acts of violence or public disorder by the presence of cameras.

Video surveillance is also believed to reduce crime by helping in the detection, arrest and prosecution of offenders. When an incident occurs in the presence of video surveillance cameras, the police can respond quickly and in a manner that is more appropriate to the situation. To the extent that offenders are captured and convicted using video surveillance evidence, this may prevent them from committing further crimes.

While video surveillance has contributed to the apprehension of criminals in a number of high-profile cases, historically its value has stemmed from its potential to deter rather than detect criminal activity. This view is now changing. The value in detecting crimes is now being considered as a primary goal of video surveillance.

Video surveillance images may also assist the police in investigating crimes. It is important to note that video surveillance footage may not only help the police identify offenders, but may also help in the identification of potential witnesses who may otherwise be reluctant to come forward.

In addition, video surveillance is believed to make people feel more safe and secure. This is an important goal of security programs for all mass transit systems. If members of the public do not feel secure, they may avoid using public transit, thereby decreasing ridership.

In short, there are reasons other than deterrence, as to why video surveillance may help to prevent crime and aid the police in criminal investigations. This may help to explain why video surveillance systems are strongly supported and continue to proliferate.

Emerging Privacy-Enhancing Video Surveillance Technology

While technology is essentially privacy neutral, if deployed without careful consideration to its impact on privacy, it may be extremely invasive. I have been a strong advocate for harnessing the strengths of technology and putting them in the service of privacy – enlisting the support of technology to enhance, instead of erode, privacy. Privacy-enhancing technologies (PETs) are those information and

communication technologies that incorporate measures to protect privacy by eliminating or reducing the collection, retention, use and disclosure of personal information. This is often referred to as "data minimization" and increasingly represents a vital component of privacy protection.

To avoid the costly and ineffective retrofitting of technology to address privacy issues after they have been implemented, it is essential that privacy protections be built directly into their design and implementation, right from the outset. This view is captured in my mantra of "privacy by design." It is incumbent upon those who wish to deploy surveillance systems to be aware of and adopt PETs whenever possible, especially as they become commercially available.

Recent research has shown that it is possible to design surveillance systems in a manner that may successfully address issues of public safety while, at the same time, protecting the privacy of law-abiding citizens.

There are a variety of technologies based on digital image processing that are currently being researched and developed for protecting the privacy of individuals appearing in video surveillance footage. As described in the research literature, these approaches are operating as follows:

> Step 1: object detection and segmentation methods for locating objects of interest, such as human faces, within images and video frames; and
>
> Step 2: object obscuration or securing methods, which, after the completion of step 1, manipulate the pixel data so that some or all viewers of the surveillance footage are unable to discern the private object content (which one is seeking to protect from viewing).

For the first step, object detection and segmentation, there are many well-established approaches using pattern recognition algorithms, some of which are currently used in surveillance and recognition systems. For the second step, object obscuration or securing, there are various approaches, the choice of which is dependent upon the application requirements. The simplest approach is to blur or discard (i.e., obscure with a black box) the private object content. The significant limitation of this approach is that the content is irretrievable for future investigative purposes if it is applied immediately during acquisition of the surveillance footage. What is needed is a novel privacy-enhancing approach that allows the personally identifiable information or objects of interest in the original video stream to be securely protected from viewing while, at the same time, preserving the original content stream and enabling this information to be retrieved at a later date, if required.

Innovative Privacy-Enhancing Approach

I am delighted to report that at the University of Toronto, Karl Martin and Kostas Plataniotis have developed such a privacy-enhancing approach to video surveillance. Their work, as described in *Privacy Protected Surveillance Using Secure Visual Object Coding*,[21] uses cryptographic techniques to secure a private object (personally identifiable information), so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key. In other words, objects of interest (e.g., a face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted. This approach represents a significant technological breakthrough because by using a secure object-based coding approach, both the texture (i.e., content) and the shape of the object (see Figure (b) below), or just the texture (see Figure (c) below) may be encrypted.[22] Not only is this approach more flexible, but the encryption used is also more efficient than existing approaches that encrypt the entire content stream. This allows designated persons to monitor the footage for unauthorized activity while strongly protecting the privacy of any individuals caught on tape. Upon capture of an incident that requires further investigation (i.e., a crime scene), the proper authorities can then decrypt the object content in order to identify the subjects in question. The decryption may be performed either in real-time or on archived footage. Since the encryption is performed in conjunction with the initial coding of the objects, it may be performed during acquisition of the surveillance footage, thus reducing the risk of any circumvention.

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

21 See Karl Martin and Konstantinos N. Plataniotis, *"Privacy protected surveillance using secure visual object coding,"* the Edward S. Rogers Sr. Dept. of Electrical and Computer Engineering, University of Toronto, Multimedia Lab Technical Report 2008.01 online: **http://www.dsp.utoronto.ca/~kmartin/papers/tech_report_2008.01-surveillance**

22 The figure contains a photograph of one of the researchers. The researcher in the photograph consented to its publication in this Report.

The Pitfalls of a Zero-Sum Approach

Over the years, I have argued that adopting a zero-sum paradigm, where one party wins and one party loses, is ultimately shortsighted and least effective. As a result, my office has developed "positive-sum" models for consideration in the use of emerging technologies, whereby both parties may "win" and neither party must, by necessity, lose. In the scenario involving video surveillance cameras, the police may have a legitimate goal in using video surveillance cameras as a tool in the detection of criminal activity, while, at the same time, individuals have a legitimate expectation that their daily activities will not be monitored and preserved on tape. The innovative work of Martin and Plataniotis provides an ideal example of a positive-sum technology, where both interests can prevail: Video surveillance cameras may be deployed for reasons consistent with public safety and law enforcement; however, no personal information from camera footage is accessible to unauthorized parties not in possession of the decryption key. Strong policies would need to be implemented in conjunction with this technology to restrict access to the decryption key to a limited number of authorized individuals. Protocols should also be developed governing the conditions under which video surveillance footage could be decrypted – for example, only after a crime had been committed or a safety mishap had occurred.

The use of this type of privacy-enhancing technology would thus allow for video surveillance to be conducted without the usual concerns associated with this type of surveillance. For the great majority of the surveillance footage, there would be absolutely no access or viewing of any personally identifiable information, and no unauthorized activities, such as viewing out of curiosity or "leering," would be possible.[23] Therefore, this privacy-enhancing technology would enable both the use of video surveillance cameras *and* privacy to co-exist, side by side – without forfeiting one for the other: positive-sum, not zero-sum.

23 See Jeffrey Rosen's seminal book *"The Naked Crowd"* (2004) for examples of video surveillance voyeurism where unsupervised video surveillance camera operators in the United Kingdom entertained themselves by zooming in on attractive young women or couples engaged in sexual activities. In this book, he argues that it is possible to strike an effective balance between liberty and security by adopting well-designed laws and technologies.

Conduct of the Investigation

As discussed above, in its letter of complaint to the IPC, Privacy International raised concerns regarding the TTC's deployment of video surveillance cameras and asserted that the TTC's use of video surveillance was not in accordance with the privacy provisions of the *Act*. Privacy International's letter made reference to past studies on the efficacy of video surveillance, technological concerns regarding the use of video surveillance, as well as legal considerations.

In order to provide the TTC with the opportunity to respond to the issues raised in the complaint, my office met with their staff. I also wrote to the TTC to confirm my understanding of the background facts pertaining to this complaint and to obtain the TTC's written representations on whether the operation of the video surveillance system was in accordance with the provisions of the *Act*. The TTC provided a thorough and detailed response. Privacy International was also provided with an opportunity to submit additional information, but declined to do so.

Staff from my office also conducted a site visit to examine the video surveillance system in place at a representative TTC subway station.

Extent of Surveillance

The TTC indicated that there are currently cameras in both the TTC's subway system and on its surface vehicles (which comprise buses and streetcars). With respect to the TTC's fleet of 1,750 surface vehicles, 286 buses are fully equipped with four cameras on each bus, for a total of 1,144 cameras. (To date, no cameras have been installed on streetcars.) With respect to the TTC's subway system, there are currently 1,200 cameras located throughout the 69 stations. These cameras are generally located at choke points (major access points), Designated Waiting Areas, automatic entrances, elevators, collector booths, and other site-specific areas of concern.

The TTC expressed its plans to expand its surveillance program on both surface vehicles and within the subway system. Specifically, the TTC plans to equip its remaining 1,464 surface vehicles with cameras so that all surface vehicles will have cameras by the end of 2008. With four cameras planned for each vehicle, this would amount to a total of 7,000 cameras on the TTC's entire fleet of surface vehicles. In addition, there are plans to install five cameras per vehicle on all 144 Wheel Trans vehicles (a total of 720 cameras) by the end of 2008. With respect to the subway system, the TTC plans to increase the number of cameras on the subway system by 1,100, from the current number of 1,200, to a total of 2,300 by the end of 2011. In addition, the TTC plans to introduce cameras inside subway cars. Currently, there are plans to install a total of 1,014 cameras on 39 new subway train sets that will begin to be introduced into the TTC system in late 2009.

It is our understanding that all of the existing and proposed cameras are or will be located in places where they have the potential to capture images of individuals.

Operation of the System

The TTC has also provided background information on the operation of the cameras. Specifically, the TTC has provided information about the retention of video surveillance images; the type of technology used; the monitoring of live video surveillance images; and access to recorded video surveillance images on both surface vehicles and within the subway system.

With respect to retention schedules, the TTC explained that recorded video surveillance images from surface vehicles are retained for a period of 15 hours, at which time they are automatically overwritten. For the cameras operating in subway stations, the recorded video surveillance images are retained for a maximum period of up to seven days, at which time they are automatically overwritten.

With respect to the type of video surveillance technology used, the TTC indicated that the cameras located on surface vehicles all utilize digital technology. The cameras currently located within the subway system utilize both analog and digital technology.

With respect to the active monitoring of the video surveillance images, the TTC stated that the cameras located on surface vehicles are not monitored nor are the images accessible by the vehicle drivers. The only way that video surveillance images from surface vehicles could be actively monitored from a remote location would be through a wireless video surveillance network. Such a network has not been installed by the TTC. With respect to the subway system, the TTC noted that, while these cameras are not generally monitored, cameras from 16 subway stations are currently linked through a fibre-optic cable that permits live remote access to video surveillance images by four departments of the TTC: Transit Control, Signals/Electrical/Communications Maintenance Department, Signals/Electrical/Communications Engineering Department, and Special Constable Services. The purposes for which each of these departments may access the live video surveillance images is described below.

With respect to Transit Control, although the live feed and monitors are "on" 24 hours a day in case a problem arises within the subway system, the video surveillance images are not actively monitored. Transit Control determines which subway platforms are monitored through the live feed. Approximately eight cameras can be displayed at one time. With respect to both Signals/Electrical/Communications Engineering and Maintenance Departments, the cameras are not actively monitored. Remote access to the video surveillance signals is used strictly for maintenance-related issues, such as system failure, camera failure, network failure or preventative maintenance. Special Constable Services also do not actively monitor the live video surveillance feed. All access is strictly logged and incident driven.

In addition to the live video surveillance feed from cameras linked to the fibre-optic cable, there is a live feed to monitors that are viewable by a TTC Superintendent on weekdays during the morning and evening rush hours. The live feed monitors the subway platforms at crossover stations, where the north-south subway line meets the east-west subway line. The live video surveillance images are used strictly for the purpose of monitoring overcrowding on the platforms to ensure passenger safety. If necessary, public announcements are made by the Superintendent to provide updates or directions to passengers.

Currently, with respect to access to recorded video surveillance images, from both surface vehicles and the subway system, when an incident has taken place, an investigator must isolate and copy the images prior to the expiration of the retention period in order to use them during the course of an investigation. The ability to access and download recorded video surveillance images is therefore strictly controlled. Investigations may be conducted internally by the TTC, or by an external law enforcement agency, such as the Toronto Police Services.

In addition, once a Memorandum of Understanding (MOU) is signed between the Toronto Police Services Board and the TTC, the Police will have direct remote access to the recorded video surveillance images collected in the subway system. All access to the video surveillance images will be incident driven and require a case file number. Access will be limited to eight individuals within the Video Services Unit. All access will be fully logged.

The TTC's operation of the video cameras is governed by its "Video Recording Policy" (the Policy), which has been provided to my office in draft form. The Policy is not yet complete and has not been officially adopted by the TTC. Once in force, the Policy will address all major aspects of the TTC's usage of their cameras, including:

- a statement of the program's rationale and objectives;
- the responsibilities of various job designations within the TTC regarding the surveillance system;
- the requirement that Notice of Collection be provided to all TTC passengers whose images are collected through the surveillance cameras;
- procedures for responding to a potential privacy breach; and
- acceptable retention periods for recorded images.

Public Consultation

The TTC stated that it has engaged in various forms of public consultation on video surveillance at different points in time. For instance, with respect to cameras within the subway system, during the design of the Sheppard Subway Extension, a Personal Security Design Review Group (PSDRG) was created in order to provide input into security features of the new subway line, including the installation of cameras. The TTC stated that the PSDRG was comprised of various public interest

groups, including the Toronto Safe City Committee and the Metro Action Committee on Public Violence against Women.

With respect to the use of video surveillance cameras in new subway cars, the TTC stated that it had conducted a public viewing of a mock-up of the new subway car from June 6 to July 21, 2006, and had invited the public to comment on its features, including the use of video surveillance cameras.

For the cameras planned on streetcars, the TTC also noted that it has been involved in a public consultation with respect to the purchase of new streetcars. Among other things, this public consultation dealt with the potential installation of video surveillance cameras. In addition, the TTC stated that recommendations relating to the purchase of additional cameras for surface vehicles have been the subject of public reports,[24] and that any group wishing to provide feedback on such reports would have the option of doing so at a TTC Commission meeting.

Issues Arising in the Investigation

I have identified the following issues arising from this investigation, each of which will be discussed in turn.

(A) Is the information collected by the TTC's video surveillance cameras "personal information" as defined under section 2(1) of the *Act*?

(B) Is the collection of personal information by the TTC's video surveillance cameras in compliance with section 28(2) of the *Act*?

(C) Is the Notice of Collection provided to passengers in compliance with section 29(2) of the *Act*?

(D) Is the disclosure of personal information to the Toronto Police Services in compliance with section 32 of the *Act*?

(E) Does the TTC have adequate security measures in place to safeguard the personal information collected?

(F) Does the TTC have proper destruction processes in place for recorded information that is no longer in use?

(G) Does the TTC have proper retention periods in place for personal information that is collected?

(H) Has the TTC undertaken all appropriate steps prior to implementing video surveillance?

(I) Is the TTC's video surveillance system subject to regular audits?

24 See the TTC website: **http://www.ttc.ca/postings/gso-comrpt/**

Issue A: Is the information collected by the TTC's video surveillance cameras "personal information" as defined under section 2(1) of the *Act*?

In order for a given record of personal information to be subject to the privacy provisions of the *Act*, it must qualify as "personal information" under the definition set out in section 2(1). Section 2(1) of the *Act* states, in part:

> "personal information" means **recorded information about an identifiable individual**, including,
>
> (a) information relating to **the race, national or ethnic origin, colour, religion, age, sex,** sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> (e) the personal opinions or views of the individual except if they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; … .
>
> [emphasis added]

The *Guidelines* state:

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*.[25]

25 See *Guidelines*, page 2.

In this case, the records at issue are the images of individuals that are captured by cameras situated within the TTC system. Clearly, such images are capable of identifying particular individuals and therefore, constitute "recorded information about an identifiable individual."

I am satisfied that the records in question qualify as "personal information" under section 2(1) of the *Act*. I note that the TTC concurs with this position.

Conclusion: The information collected by the TTC's video surveillance cameras qualifies as "personal information" as defined under section 2(1) of the *Act*.

Issue B: Is the collection of personal information by the TTC's video surveillance cameras in compliance with section 28(2) of the *Act*?

In its letter of complaint to the IPC, Privacy International focused on the issue of whether the TTC's collection of personal information through the video surveillance cameras was permissible under the *Act,* and stated:

> In this complaint we argue that the collection principles are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers.

The section of the *Act* that addresses the collection of personal information is section 28(2), which establishes a basic prohibition on the collection of personal information, but states that there are three circumstances under which the collection of personal information may take place. Section 28(2) states:

> 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.

In order for a particular collection practice to be in accordance with the *Act,* it must be shown to satisfy at least one of the three conditions set out in section 28(2). In other words, the institution must show that the collection of personal information is either, (1) expressly authorized by statute, (2) used for the purposes of law enforcement, or (3) necessary to the proper administration of a lawfully authorized activity.

The first step in the section 28(2) analysis is to address whether any of the above conditions apply to a given collection of personal information. In this case, the TTC has not provided reference to a statute that provides the express authorization for the collection of personal information through video surveillance. Accordingly, the first condition does not apply.

With respect to the remaining two conditions, in its letter of complaint to the IPC, Privacy International stated that the primary area of focus should be the third condition, which can also be referred to as the "necessity condition." In its letter, Privacy International made reference to the Ontario Court of Appeal's decision in *Cash Converters Canada Inc. v. Oshawa (City)*[26] (*Cash Converters*) in stating:

> We understand that this is arguably a law enforcement activity and therefore legal exemptions exist for some data privacy principles, as under s.28(2) of MFIPPA. Recently the Ontario Court of Appeal ruled, in *Cash Converters Canada Inc. v. Oshawa (City),* that where identifiable information is made available to the police it must first meet the necessity condition "where the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity". When it is possible to find other ways of achieving the stated lawful goals then the institution must choose another route. We do not believe that the TTC has adequately addressed the necessity of this information collection and has not considered access policies.

While the necessity condition is certainly applicable to this investigation, an additional condition that should be considered is the second condition of 28(2), which permits the collection of personal information that is used for the purposes of law enforcement (the law enforcement condition). In the *Cash Converters* decision, the law enforcement condition was not applicable because the collection of personal information at issue was a collection pursuant to a municipal by-law of the City of Oshawa. Under Ontario's *Municipal Act,* a municipality is not permitted to enact a by-law for the purpose of law enforcement. Therefore, consideration of the second condition was not an option. That is not the case in the present investigation.

I will now proceed to consider the application of both the necessity condition and the law enforcement condition in section 28(2) of the *Act*.

Necessary to the Proper Administration of a Lawfully Authorized Activity (The Necessity Condition)

In *Cash Converters*, the Ontario Court of Appeal adopted the approach my office has taken in the past with respect to the application of the necessity condition and stated:

> In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the *Act*. Similarly, where the

26 2007 ONCA 502.

> purpose can be accomplished another way, the institution is obliged to choose the other route.[27]

Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the "lawfully authorized activity" in question, and second, it must demonstrate how the collection of personal information is "necessary," not merely helpful, to the achievement of this objective. In addition, this justification must be provided for all classes of personal information that are collected.

In this case, the "activity" in question is the operation of a public transit system by the TTC. The TTC is lawfully authorized to operate under Part XVII of the *City of Toronto Act*, *2006,* which provides that the TTC has the exclusive authority to establish, operate or maintain "a local passenger transportation system within the City." Therefore, in order to satisfy the necessity condition under section 28(2), the TTC must demonstrate that its collection of personal information through use of video surveillance cameras is necessary to the proper operation of a public transportation system within the City of Toronto.

In considering whether the necessity condition has been satisfied, I have reviewed the documentation provided by the TTC, the information contained in the letter of complaint provided by Privacy International, and the research on the topic discussed earlier in this Report. In addition, during the course of the investigation, my office found additional information pertaining to video surveillance in mass transit systems, which I have also taken into consideration in determining the necessity of the collection. All of this documentation is discussed below.

Video surveillance is not a new phenomenon in mass transit systems. For years, public transit systems in North America have relied on video surveillance cameras to improve their operations and to enhance public safety and security.

It has been widely recognized that safety and security are essential to the proper functioning of mass transportation systems.[28] Six relevant goals have been proposed for any mass transit security system:

- Awareness of the risks to employees and users of the system, including the nature, level and impact of each risk;
- Mitigation of each risk to the greatest extent possible and an understanding of the nature of any unmitigated risks;

27 *Ibid*, at para. 40.

28 See, for example, B.M. Finn, *"Keeping an Eye on Transit,"* The Institute of Electrical Engineers, 2004 and Michael Greenberg, *"The need for closed circuit television in mass transit systems,"* Law Enforcement Executive Forum. 6(1), 2006 online: **http://www.umaryland.edu/healthsecurity/docs/CCTV%20in%20Mass%20Transit%20Systems.pdf**

- Awareness of all threats to the proper functioning of the system and mitigating those risks to the greatest extent possible;
- Development of appropriate responses to risk events, both during and after such events;
- Understanding the perceptions and concerns of employees, users, and potential users of the system; and
- Responding to concerns about safety and security through actions and communications.[29]

Typically, mass transit systems have multiple locations, are distributed over large areas, are complex, and have a high volume of passengers. These features of transit systems conspire to make it extremely difficult to achieve the necessary safety and security goals. Video surveillance is viewed as an essential tool for helping to fulfill some of these security goals. Video surveillance is said to serve a number of key functions within mass transit systems, namely:

- Prevention of accidents by monitoring overcrowding, monitoring of individuals in dangerous situations, and monitoring of individuals who may be a danger to themselves;
- Organization of the movement of individuals to avoid bottlenecks and to ensure smooth passenger flows;
- Prevention of crime, public disorder and terrorist acts by monitoring crowd and individual behaviour, and directing security personnel; and
- Assisting in the investigation of incidents by determining how they occurred, identifying potential offenders and witnesses; and providing evidence of criminal or possible terrorist activities.[30]

With respect to the TTC in particular, the Operator Assault Task Force, consisting of representatives of the TTC and the Amalgamated Transit Union Local 113 , was created in 2002 in response to statistics indicating an increase in the number of operator assaults in the Toronto transit system. In 2005, the Task Force issued a report that recommended the implementation of video surveillance cameras on all buses and streetcars to assist in preventing operator assaults.[31]

On January 28, 2008, a major newspaper, the *Toronto Star,* reported on an investigation into the impact of work-related stress on TTC bus, streetcar and subway

29 See B.M. Finn, *"Keeping an Eye on Transit,"* The Institute of Electrical Engineers, 2004, page 12.

30 *Ibid*, page 13.

31 See the TTC's *"Operator Assault Task Force Report of Findings,"* 2005.

operators.[32] During the *Toronto Star* investigation, the reporters obtained information about occupational injury and disease reports filed with the Workplace Safety and Insurance Board, over a five-year period ending in 2005. The investigation, which included interviews with TTC drivers, revealed that at least 181 drivers had filed claims for post-traumatic stress disorder, missing an average of 49 days of work. Post-traumatic stress disorder, associated with the witnessing or experiencing of a traumatic event involving the threat of injury or death, was found to be the second leading cause of lost workdays at the TTC. Drivers were found to have suffered a wide range of abuse on the job – being shot at, spat on, punched, headbutted, slashed with broken bottles, swarmed, kicked and beaten, to name a few examples. The rate of post-traumatic stress disorders among drivers was found to be four times higher than that of Toronto police officers. An additional 102 TTC operators reported missing weeks or months of work due to anxiety, neurotic disorders, and depression. TTC operators were found to report these disorders more often than any other workers in Ontario. The *Toronto Star* investigation also revealed that the number of reported crimes on TTC property had increased dramatically, from 2,744 in 2005 to 3,415 in 2006 – an increase of 24 per cent.

As part of the critical infrastructure of modern societies, it is generally accepted that mass transit systems are viewed as highly desirable targets for terrorists. Consequently, in addition to dealing with operator assaults and crime at the local level, mass transit systems have found themselves more recently in a position of having to address issues of national security. Accordingly, video surveillance cameras within mass transit systems are being upgraded and expanded to deal with the increased potential of a terrorist threat.

On March 20, 1995, subways in Tokyo, Japan, were the target of a poison gas attack, an act of domestic terrorism perpetrated by members of Aum Shinrikyo.[33] In five coordinated attacks, the perpetrators released sarin gas on several lines of the Tokyo Metro, killing 12 people, severely injuring 50, and causing vision problems for nearly 1,000 others. The attack was directed against trains passing through Kasumigaseki and Nagatacho, home to the Japanese government.

More recent high-profile attacks on public transit systems in Europe underscore this potential terrorist threat. In March 2004, there was a series of coordinated bombings against the commuter train system of Madrid, Spain, killing 191 people and wounding 1,755. On July 7, 2005, there was a series of coordinated terrorist bomb blasts that hit London's public transport system during the morning rush

32 See the *Toronto Star*, *"TTC drivers in crisis: Star investigation finds frequent abuse at work puts them at high risk of stress disorder,"* January 21, 2008.

33 Aum Shinrikyo was a religious organization that turned to terrorist tactics, apparently to hasten the apocalypse.

hour. At 8:50 a.m., three bombs exploded within 50 seconds of each other on three London subway trains. A fourth bomb exploded on a bus nearly an hour later, at 9:47 a.m. in Tavistock Square. The bombings killed 52 commuters and four suicide bombers, injured 700, and caused disruption of the city's transport system (severely for the first day), as well as immobilizing the country's mobile telecommunications infrastructure.

With respect to the TTC, in 2004 there were two national security investigations involving activities within the Toronto subway system. At that time, upgrades to the TTC security system were recommended by the Chief of the Toronto Polices Services. This recommendation was supported by the Royal Canadian Mounted Police (RCMP) Integrated Security Enforcement Team. In addition, an independent security consultant had recommended the implementation of a system-wide surveillance system for each station and all subway cars following a terrorism-specific risk and vulnerability assessment of the TTC.

The reports, studies and investigations discussed above provide compelling evidence that public safety and security needs on mass transit systems in general, and operator assaults and crime within Toronto's public transit system in particular, represent a pressing and substantial societal concern. I will now proceed to assess whether video surveillance would, in fact, address this pressing and substantial societal concern.

In May of 2001, prior to the terrorist events on September 11th, the National Center for Transit Research issued a report outlining the results of a survey of transit agencies throughout the United States with respect to the issue of operator assaults and public safety.[34] Of the 32 agencies that responded to the survey, the majority (26) reported having some type of surveillance system in place. Surveillance cameras in public transit systems were found to be implemented for one or more of the following reasons:

- Crime prevention and response
- Risk management
- Response to events in progress
- Customer service
- Employee security and other employee-related issues
- Legal evidence

34 See Patricia Maier and Jud Malone, *"Electronic surveillance technology on transit vehicles: a synthesis of transit practice,"* Transit Cooperative Research Program, TCRP Synthesis 38, 2001 online: **http://onlinepubs.trb.org/onlinepubs/tcrp/tsyn38.pdf**

By far, the great majority of transit agencies that used video surveillance (all but one surveyed) indicated that they would recommend the technology to other agencies. Agencies that responded to questions about the effectiveness of surveillance in reducing incidents of crime, rated their systems as being above average. Many reported measurable reductions in the number of assaults and incidents of vandalism. In response to the question relating to the effectiveness of surveillance in achieving criminal convictions, agencies rated their systems as being somewhat better than average. The majority of agencies also reported increases in both riders' and operators' perceptions of security linked to the use of video surveillance.

The TTC conducted a survey of 26 transit agencies in North America regarding the use of video surveillance cameras on transit vehicles.[35] The vast majority of the transit agencies that participated in the survey reported very positive outcomes with video surveillance, including the following: dramatic decreases in crime, reductions in operator and customer assaults, reductions in fraudulent insurance claims, reductions in complaints, improved perceptions of security, the identification, apprehension, and prosecution of suspects in criminal investigations, and the control of student behaviour problems.

In order to determine the use and effectiveness of the existing video surveillance cameras in the Toronto subway system for investigating crimes, the TTC examined requests from law enforcement investigators for information, during the period from January 2007 through July 2007.[36] The study found that 86 per cent of the law enforcement investigators who responded reported that the video images provided positive investigative value. Further, 38 per cent of the respondents indicated that the suspect or suspects caught on camera were successfully apprehended as a result of the images that had been retrieved through the video surveillance cameras.

In the United States, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen their nation's rail and transit systems, including offering grants to state and local governments for programs and equipment to help manage this risk. Training and deploying manpower and assets for high-risk areas, developing and testing new technologies, and performing security assessments of systems across the country are other measures being taken by the department. Similarly, the Canadian government has also allocated funding for transit security that will "improve security for all who use urban transit in Canada."[37] Video surveillance is viewed as one of the mechanisms of a broader program to address these security issues on mass transit systems.

35 A copy of the report on this evaluation was provided to the IPC in the TTC's representations.

36 A summary of this research was provided to the IPC in the TTC's representations.

37 See Transport Canada's news release, *"Canada's new government invests $37 million to improve transit security in six urban areas,"* November 14, 2006, available online: **http://www.tc.gc.ca/mediaroom/releases/nat/2006/06-h138e.htm**

The United States government's funding for security programs and state and local government use of these funds for video surveillance programs was the subject of a DHS workshop held on December 17-18, 2007. The department was seeking input into best practices for states that receive funding for video surveillance installations that would assist the government in ensuring the protection of privacy and civil liberties. A broad range of perspectives were represented at the conference, held in Washington, D.C. On one side of the spectrum, civil liberties groups argued that public video surveillance systems threatened privacy, especially when used in combination with other technologies (e.g., data mining, GPS tracking, RFID, Internet, heat sensing video), and have a real potential to change the relationship between the public and the government.[38] On the other side of the debate, law enforcement and emergency management groups noted the need for video surveillance as a key tool to deter criminals; support apprehension and investigation; increase perceptions of safety; promote commerce; and aid in prosecutions.

Interestingly, however, one of the areas in which there was general agreement and acceptance of video surveillance was in the area of mass public transit. The view was that in light of the extensive areas involved (tunnels, platforms, stairways), the high numbers of passengers (especially during rush hours) and the around-the-clock operating hours of the system, the ability to deal with security issues could not feasibly be limited to increasing the number of security personnel. It was widely acknowledged that one or more cameras could easily cover far more territory than one human being. Similarly, there was general agreement that it would be extremely cumbersome (and impractical) to install a screening mechanism like those existing in airports. Consequently, the views of both privacy advocates and those in emergency management and law enforcement converged on the need for video surveillance in urban mass transit systems – all agreed that the use of video surveillance cameras in this context was justifiable.[39]

There was also another use of video surveillance that did not appear to be particularly objectionable to civil libertarians and privacy advocates, namely the use of such surveillance for the purpose of workplace safety. As noted above, workplace safety, particularly with respect to operator assaults, has been a key issue for the TTC.

Consistent with the views expressed above, there is also evidence to suggest that the general public recognizes that video surveillance may be justifiable in certain high-risk locations and that there is a difference between real-time versus archived video surveillance. For example, in one study conducted by Christopher Slobogin,

38 See Mark Scholosber and Nicole A. Ozer, *"Under the watchful eye: the proliferation of video surveillance systems in California,"* The California American Civil Liberties Union Affiliates, August 2007, online: **http://www.aclunc.org/docs/criminal_justice/police_practices/Under_the_Watchful_Eye_The_Proliferation_of_Video_Surveillance_Systems_in_California.pdf**

39 Conclusions based on extensive discussions with Washington conference panelists.

190 people who had been called for jury duty in Gainesville, Florida, were presented with 20 scenarios of video surveillance by the police.[40] The subjects were asked to assume that the target of the surveillance was innocent of any criminal activity. They were then asked to rate the "intrusiveness" of the surveillance on a scale of 1 to 100, with 1 being "not intrusive" and 100 being "very intrusive." Subjects rated the video surveillance of national monuments and transportation centres, such as airports and train stations, as being minimally invasive (M=20). On average, video surveillance of streets with the tapes destroyed after 96 hours was rated slightly above the middle on the intrusiveness scale (M=53), while street surveillance without the destruction of tapes was rated as being significantly more intrusive (M=73). This supports the position that the public may not view video surveillance in mass transit systems as being unreasonable, especially if the tapes are destroyed within a reasonable time frame. This study is relevant in the context of the present investigation since the TTC does not actively monitor live video surveillance images and recorded video surveillance images are destroyed after a short retention period, unless they are used for an investigation. Thus, the type of video surveillance being undertaken in the Toronto transit system seeks to minimally impact privacy rights, and may not be perceived as being highly invasive by the general public.

The TTC also noted that the use of video surveillance cameras by transit authorities is quite common, not only in Canada, but around the world. With respect to Canada, the TTC provided information demonstrating that the transit authorities in both Montreal and Vancouver are deploying rail-based video surveillance systems that are far broader in scope than what is being planned for the TTC's subway system.[41]

In its letter of complaint to the IPC, Privacy International stated, with respect to the TTC's video surveillance system, "that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers." I have considered these claims in light of the materials provided by the TTC in response to this complaint and the other documentation cited in this Report. I will address the issues of privacy protocols and access powers in the latter sections of this Report.

To support its position that the collection of information through video surveillance in the Toronto public transit system is unnecessary and disproportionate, Privacy International has disputed the TTC's claim that the expanded video surveillance system would reduce the incidence of crime, while also improving counter-terrorism measures. Specifically, Privacy International referred to a report on a pilot

40 Slobogin, Christopher, *"Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity,"* Mississippi Law Journal, Vol. 72, 2002, online: **http://ssrn.com/abstract=364600**

41 The research was summarized in the TTC's representations to the IPC.

project launched in the Berlin underground.[42] An interim report on the effectiveness of the scheme found that video surveillance did not reduce the incidence of criminality, but rather led to a small increase.

After reviewing an English translation of this study, I noted a number of shortcomings: the time frame for the evaluation of the pilot project was extremely short (i.e., five months); while video surveillance may not have reduced the rate of crime, it was successful in achieving other safety and security objectives, such as documenting attacks on employees. Recall that the objectives of video surveillance in mass transit systems are multifaceted, going beyond finding reductions in crime. Further, the challenges in finding statistically significant reductions in crime rates, in any particular evaluation study, have already been discussed at length earlier in this Report.

Privacy International also pointed to research conducted in the United Kingdom to demonstrate the lack of effectiveness of video surveillance in preventing crime and providing investigatory evidence. While I agree that video surveillance may not be a "silver bullet" in this regard, I again note that there are broader goals for its use in mass transit systems and that, given the massive scope of such systems, there are few viable alternatives. A combination of measures, each with their own recognized limitations, is, in my view (and that of many security experts), the best option for potentially achieving the broad safety and security objectives of mass public transit systems.

Underlying much of the information provided by the TTC is the notion that mass transit systems have specific security requirements that give rise to the need for video surveillance. Since mass public transit often involves the movement of large numbers of passengers in small spaces, the risks to passenger security may be easily distinguished from those in outdoor public spaces.

In addition to security, mass transit systems are also concerned with passenger health and safety, operator safety, and crowd control issues that arise from large numbers of passengers on the system. Accordingly, in considering a threshold to determine whether the use of video surveillance is necessary, I am cognizant of the unique and multifaceted needs of mass transit systems such as the TTC.

The documentation reviewed indicated that there is widespread perception among transit system operators and the general public that video surveillance systems are useful in preventing crime and aiding in criminal justice processes. There is also a growing body of empirical evidence to suggest that video surveillance systems may be an effective part of a crime prevention and national security strategy,

42 See the article *"Study shows video surveillance on the Berlin underground has not improved safety,"* Heise Online, October 10, 2007 available online: **http://www.heise.de/english/newsticker/news/97168**

aiding in police investigations. In addition, transit system security experts and national security experts continue to strongly recommend the use of video surveillance systems as one component of a comprehensive security strategy for mass transit systems. I have taken all of these factors into consideration in assessing whether or not the TTC has sufficient justification for expanding its use of video surveillance.

In my view, safety and security are essential components to the proper functioning of the Toronto public transit system. In order to preserve the safety and security of the system, the TTC must address not only the growing issues of operator assaults, crime on the TTC, and the potential threat of terrorism, but especially the challenge of moving hundreds of thousands of passengers safely and quickly, on a daily basis. Given the nature of the safety and security needs, and the massive scope and complexity of the public transit system in the City of Toronto, achieving these goals through a combination of other measures (e.g., increased security personnel, enhanced lighting) would not be feasible. The best strategy would be to employ the full range of safety and security options available, which would include video surveillance.

Finally, to return to the test expressed by the Ontario Court of Appeal in *Cash Converters*, in order for a given collection of personal information to satisfy the necessity condition:

> … the institution in question must demonstrate that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the *Act*.

In this case, the sole class of personal information at issue is the images of individuals that are passengers on the TTC system. Based on the foregoing, I am satisfied that the collection of individuals' images is not merely helpful, but is also necessary to the proper administration of the TTC. Accordingly, I am satisfied that the collection of personal information through the use of video surveillance cameras meets the necessity condition, and is therefore in compliance with section 28(2) of the *Act*.

Used for the Purposes of Law Enforcement (Law Enforcement Condition)

Although I have concluded that the TTC's collection of personal information through video surveillance satisfies the necessity condition (i.e., that it is necessary to the proper administration of a lawfully authorized activity), and is therefore permissible under section 28(2) of the *Act*, I will now proceed to consider whether the collection would also be upheld under the law enforcement condition (i.e., that it is used for the purposes of law enforcement).

The TTC has stated that the images collected through its video surveillance system are used for the purposes of law enforcement, and has made reference to the activities of staff working in the TTC's Special Constable Services Department, who are the primary users of the recorded images collected through the surveillance system.

The definition of "law enforcement" is contained in section 2(1) of the *Act*, which states:

> "law enforcement" means,
>
> (a) policing,
>
> (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
>
> (c) the conduct of proceedings referred to in clause (b);

With respect to the role of staff working in Special Constables Services Department, the TTC has stated:

> … the employees within our Special Constable Services Department have been granted "special constable" status by the Toronto Police Services Board and the Solicitor General. As such, special constables have been conferred the powers of a police officer for specific purposes, including enforcing the Criminal Code throughout the transit system.

The TTC's description of the powers of a "Special Constable" are supported by section 53 of the *Police Services Act*, which states, in part:

> (1) With the Solicitor General's approval, a board may appoint a special constable to act for the period, area and purpose that the board considers expedient.
>
> …
>
> (3) The appointment of a special constable may confer on him or her the powers of a police officer, to the extent and for the specific purpose set out in the appointment.
>
> …

In addition to the *Police Services Act,* further details about the status of TTC Special Constables may be found in a May 9, 1997 Agreement (as amended) between the Toronto Police Services Board (the Board) and the TTC, which sets out the powers, jurisdiction and certain procedures of the TTC Special Constables.

TTC Special Constables may enforce various federal and provincial statutes, including the federal *Criminal Code* and related drug and controlled substances legislation, the provincial *Mental Health Act, Trespass to Property Act, Liquor Licence Act* and specified sections of the *Provincial Offences Act*. In addition, TTC Special Constables may enforce TTC By-Law #1, which sets out the rules that passengers are required to follow to promote, among other goals, public safety and security. For example, the by-law provides that:

> No person shall commit any nuisance, disturb the peace, or act contrary to public order, in or upon any vehicle or premises of the Commission.
>
> No person shall carry, nor shall the Commission be required to carry on any vehicle, any goods which are of an offensive, dangerous, toxic, flammable or explosive nature that are likely to alarm, inconvenience, cause discomfort, or injure any person, or cause damage to property, whether or not such goods are contained in an approved container, without authorization.

The jurisdiction of the TTC Special Constables is subject to geographic restriction. TTC Special Constables' jurisdiction is limited to properties and vehicles under TTC control, and all facilities and leased/rented properties affiliated or associated with the TTC, within the City of Toronto. Additionally, if an offence originates on, or is in relation to, TTC property, a TTC Special Constable may investigate such an offence within the City of Toronto.

The Agreement also sets out procedures relating to the investigative authority in certain situations and with respect to certain offences between the Police and TTC Special Constables. For example, if a Police officer and a TTC Special Constable both attend a call within the geographic jurisdiction of the TTC, or if a dual procedure or indictable offence is involved (i.e., those offences of a more serious nature), TTC Special Constables must take instruction and direction from Police. If the alleged offence is not a dual procedure or indictable offence, the TTC Special Constables shall proceed to conduct the investigation. The Agreement further provides that the Police have primary responsibility for responding to and investigating serious occurrences on the transit system (e.g., violence involving weapons, violent incidents where injury has occurred or is likely to occur), while TTC Special Constables may respond to minor physical assaults not involving weapons or verbal confrontations. Finally, the Agreement provides that, for a specified list of offences that includes robbery, weapons, drugs, explosives and sexual offences, amongst others, the Police must be called and may investigate. The Police need not be called, however, where the alleged offence involves theft under $5000.

The Agreement provides that the TTC Special Constables shall be trained by the TTC in accordance with training standards prescribed by the Board for members

of the Police, as modified for the TTC Special Constables considering their powers, duties and responsibilities.

Other factors which I find relevant include the following: TTC Special Constables may have access to confidential police information, such as CPIC and criminal record information; TTC Special Constables, although prohibited from carrying weapons and carrying out vehicle pursuits, may carry "pepper spray;" TTC Special Constables may make arrests and must transfer persons detained in custody to police; every arrest and investigation of a criminal offence conducted by a TTC Special Constable must be reported to the police.

Finally, the TTC must establish a complaints investigation procedure regarding the conduct of TTC Constables that corresponds to that of the Police, and must provide the Board with the results of all complaints investigations, as well as any information concerning misconduct or alleged misconduct. The Board may, if provided with a finding of misconduct or information regarding misconduct, suspend or terminate the appointment of a TTC Special Constable.

Considering the foregoing, and in particular the authority under section 53 of the *Police Services Act* and the powers, jurisdiction and procedures set out in the Agreement between the TTC and the Board, I am satisfied that the TTC Special Constables engage in "policing" and thus meet the definition of "law enforcement" under the *Act*. Although in certain contexts, the status and authority of the TTC Special Constables may be construed as subordinate to that of the Police, I nevertheless find that their activities are sufficiently similar to the Police such that they come within the meaning of "policing" under the "law enforcement" definition.

Finally, I am satisfied that when the video surveillance system is accessed on an incident driven basis to pursue an investigation by the TTC Special Constables it is "used for the purposes of law enforcement" and the underlying collection is therefore in compliance with the law enforcement condition of section 28(2).

Section 28(2) – Conclusion

I note that a given collection of personal information is permissible under the *Act* where it may be justified under at least one of the section 28(2) conditions. Based on the foregoing, I am satisfied that the collection of personal information through the video surveillance system is permitted under two of the section 28(2) conditions. The general collection is satisfied by the necessity condition, as well as the law enforcement condition with respect to the activities of the TTC Special Constables.

Having reached the conclusion that the collection of personal information through the use of video surveillance is permissible under section 28(2) of the *Act,* it is incumbent upon the TTC to govern its video surveillance system in a manner that places a high regard on the privacy of its passengers. While TTC passengers may

accept a certain degree of surveillance, they should not expect that their images or personal information will be improperly recorded or misused for purposes that are secondary to the purposes of safety and security. Therefore, for the remainder of this Report, I will focus on the governance aspects relating to the TTC's use of video surveillance cameras.

Conclusion: The collection of personal information by the TTC's video surveillance cameras is in compliance with section 28(2) of the *Act*.

Issue C: Is the Notice of Collection provided to passengers in accordance with section 29(2) of the *Act*.

Section 29(2) of the *Act* states:

> If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

This section requires that institutions collecting personal information provide individuals with the Notice of Collection that is prescribed in section 29(2) of the *Act*. In the case of video surveillance programs, the *Guidelines* elaborate on the statutory requirement to provide a Notice of Collection and state:

> 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. Signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system, and can include an address, telephone number, or website for contact purposes.[43]

The *Guidelines* further state that while signs should contain the basic information relaying that individuals are under surveillance, the remainder of the notice requirement may be satisfied by having the entire notice appear in other media, such as in pamphlets and other printed materials.

43 See *Guidelines*, page 7.

With respect to the TTC's video surveillance program, the TTC's Policy contains the requirement that, "The TTC shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the location being video recorded." The Policy further states that the notice provided on the signs must contain the full notice requirement as set out in section 29(2) of the *Act*.

An appendix to the TTC's Policy contains an illustration of the signs, which include a picture of a camera and the following text:

> This area is being Video Recorded for Security Purposes.
>
> The personal information collected by the use of video equipment at this location is collected under the authority of the City of Toronto Act, 2006 and the *Occupiers' Liability Act*.
>
> Any questions about this collection can be directed to the Coordinator, Freedom of Information/Records Management, at [phone number and contact information].

With respect to surface vehicles, the TTC has stated that a Notice of Collection decal containing the above wording has been posted on all vehicles in which cameras have been installed. With respect to the subway system, the TTC has acknowledged that signage containing the above wording has not yet been installed, but that plans are underway to install a total of 761 signs throughout the 69 stations. The TTC plans to install the signs as the use of video surveillance cameras expands.

I am satisfied that the Notice of Collection, as drafted, meets the requirements set out in section 29(2) of the *Act* and the *Guidelines*. I am also satisfied that the TTC's plans with respect to the number and placement of signs are appropriate. However, it is imperative that the TTC ensure that signs are installed prior to the video surveillance cameras being activated at a particular site, and I will recommend that my office be advised of such developments.

Conclusion: The Notice of Collection provided to TTC passengers is in compliance with section 29(2) of the *Act*.

Issue D: Is the disclosure of personal information to the Toronto Police Service in accordance with section 32 of the *Act*?

The TTC has acknowledged that recorded video surveillance images collected from both surface vehicles and the subway system are disclosed to the Toronto Police Service (the Police) in response to requests for information about incidents involving criminal investigations. In addition, the TTC has stated that, in the future, the Police will have the ability to remotely access video surveillance images obtained from some of the cameras in the subway system, in accordance with the

MOU to be signed. The TTC provided a copy of the draft MOU to my office and indicated that the MOU would be signed once it is passed by the Toronto Police Services Board. This remote access by the Police also constitutes a disclosure of personal information on the part of the TTC, under the *Act*.

The rules relating to the disclosure of personal information are set out in section 32 of the *Act,* which states, in part:

> An institution shall not disclose personal information in its custody or under its control except,
>
> (a) in accordance with Part I;
>
> (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
>
> (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> …
>
> (g) if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
>
> …

Section 32 establishes a basic prohibition on the disclosure of personal information, but states that there are certain circumstances under which the disclosure of personal information is permissible. In order for a given disclosure of personal information to be allowed under the Act, the institution in question must demonstrate that the disclosure in question is in accordance with at least one of the statutory exceptions set out in section 32. The TTC has cited various section 32 provisions to support its position that the disclosure to the Police is permissible.

In this case, there are generally two different types of disclosures of personal information taking place. The first is the physical disclosure of personal information to the Police (or another law enforcement agency) in response to an incident which may lead to criminal charges. The second type of disclosure is that which results from the direct remote access to video surveillance images of the TTC subway system by the Police.

With respect to the first type of disclosure, the physical disclosure of recorded video surveillance images to law enforcement officials in response to a specific incident, I note that these images may be taken from cameras located in both the subway system and on surface vehicles (including streetcars, once installed).

The TTC's Policy describes the manner in which recorded images collected from the video surveillance cameras in both surface vehicles and the subway system are provided to law enforcement officials, in response to a specific incident:

> If access to a video recording record is required for the purpose of a law enforcement investigation, the requesting Officer (or in emergency situations, the Operator that authorized the release) must complete the TTC's Law Enforcement Officer Request Form … and forward this form to the [Designated Departmental Management Staff] or designate [who] will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer.

In my view, this type of disclosure of personal information, in response to a specific incident, where the requesting officer completes the prescribed form indicating a specific date, time and location of the incident being investigated, would constitute a "disclosure to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result," within the meaning of section 32(g) of the *Act*. Accordingly, I am satisfied that such disclosures are permissible under the *Act*.

The second type of disclosure (based on direct remote access to video surveillance images by the Police) is the subject of an MOU that has been drafted, but yet to be signed between the Toronto Police Services Board and the TTC. The draft MOU specifies that remote access to the video surveillance images shall only be permitted for law enforcement or public safety purposes and that no other uses are permitted without the express written consent of the TTC. The TTC stated that the remote access would take place from a computer, located within Police headquarters, connected to the TTC's subway system through a fibre-optic cable. Access to the video surveillance images will be incident driven, requiring a case file number. Access will also be restricted to only eight designated individuals, within the Video Services Unit.

The initial draft of the MOU provided to my office indicated that the Police would have remote access to both live and recorded video surveillance images. My office was concerned that access to the live video surveillance feed by the Police could lead to potentially invasive activities and improper surveillance. During the course of the investigation, the TTC revised the draft MOU to restrict the Police's remote access to recorded images only. Since the recorded images are only retained for a short period of time, I have less concern with this type of disclosure to the Police.

However, to ensure that each disclosure of personal information to the Police is for legitimate law enforcement and public safety purposes, all disclosures of personal information must be subject to stringent accountability and oversight. Accordingly, I recommend that prior to providing the Police with direct remote access to the recorded video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures to the Police be subjected to regular audits, conducted on behalf of the TTC. The TTC should provide my office with a copy of the revised draft MOU prior to signing.

Conclusion: The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the *Act*.

Issue E: Does the TTC have adequate security measures in place to safeguard the personal information collected?

Regulation 823, made pursuant to the *Act,* addresses the general security requirements for records in the custody of an institution. Section 3 of Regulation 823 states:

(1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

(2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.

(3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

The *Guidelines* elaborate on the security responsibilities of institutions operating video surveillance systems and state, in part:

- 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 labelled with a unique, sequential number or other verifiable symbol.
- Access to the storage devices should only be made by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Electronic logs should be kept where records are maintained electronically.[44]

44 See *Guidelines*, page 8.

Under the section dealing with an institution's video surveillance policy, the *Guidelines* state:

> 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.[45]

Privacy International stated that there has been "insufficient consideration regarding access powers" on the part of the TTC. My office understood this comment to mean that Privacy International is of the view that, in implementing its video surveillance cameras, the TTC did not incorporate sufficient controls over who would have access to the live and recorded video surveillance images. With due respect, I disagree with this assertion. In materials provided to my office, the TTC described the security measures put in place to prevent unauthorized access to the images obtained through the video surveillance system.

With respect to the cameras located in TTC surface vehicles, the TTC noted that the hard drives containing the recorded video images are only accessible through the use of a password, which is only available to a limited number of TTC supervisors. The operators of TTC vehicles do not have any access to the recorded video images. The TTC stated:

> In order to access, view and/or record extracted data a separate computer is required and can only be performed by authorized TTC personnel. To remove a recorder from a vehicle requires a special tool key, which is not available to operators. … In addition, if a camera is moved, altered or in any way tampered with, the recorder creates an internal log indicating the occurrence and the time.

The TTC also provided a copy of a document entitled, *Interim TTC Protocol for Surface Vehicle Safety Camera System,* which documents the manner in which access may be granted to the recorded images collected by cameras located in surface vehicles in response to specific investigations.

The TTC has similar measures in place relating to the cameras located on the subway system. The TTC provided my office with a copy of written procedures describing the TTC's internal process for requesting images recorded at a given site

45 See *Guidelines*, page 5.

within the subway system. These procedures describe the way in which recorded images may be used internally, the staff designations who may have access to them, and the manner in which access may be provided. The TTC also noted that all designated staff permitted access to recorded images must receive training on privacy and security:

> All TTC personnel that access recorded video images are required to log all activities relating to such access, including the time and purpose. A log book is maintained within each station … [E]ach recorder also creates its own internal log every time the recorder is accessed or an image is accessed.

Further, the TTC has stated:

> Cameras located within a specific subway station simultaneously transfer images to a recorder located within a secure room and area of the subway station. All recorders are in a locked cabinet, in a restricted access room.

In my view, the security measures in place, based on the information contained in the TTC's Policy, the written procedures, as well as other information provided, are comprehensive. However, I note that the TTC's Policy does not contain the requirement, as set out in our *Guidelines*, that all employees dealing with the video surveillance system must sign written agreements regarding their duties under the Policy and the *Acts*, including an undertaking of confidentiality. Accordingly, the TTC should amend the Policy to incorporate such wording to fully satisfy its responsibilities relating to security of recorded information under Regulation 823 and the *Guidelines*.

Conclusion: The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

Issue F: Does the TTC have proper destruction processes in place for recorded information that is no longer in use?

As discussed above, Regulation 823 requires that institutions have proper security safeguards in place to protect records from unauthorized access. The principle that unauthorized access should be prevented applies to all aspects of a record's life cycle, up to, and including, its destruction.

The *Guidelines* address the destruction of records that have been created through the use of video surveillance in the past and state:

> Old storage devices must be securely destroyed in such a way that the personal information cannot be reconstructed or retrieved. Destruction methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.[46]

In sum, the *Guidelines* recommend the secure destruction of all recorded video images.

With respect to the images collected from surface vehicles, the TTC stated that the system is designed to automatically overwrite every 15 hours. Since actual recording only takes place when the vehicle is in operation, the images will be deleted and overwritten with new images at least every 24 hours.

The TTC's Policy addresses the secure destruction of video records, and states:

> The TTC will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

In addition to the general destruction requirements expressed in the Policy, the TTC has also provided specific information on the secure destruction of recorded images. With respect to images taken from recorders located on surface vehicles, the TTC stated:

> If a request for images is received, the images are downloaded from the digital video recorder to an investigation station (laptop computer). If the images are to be retained, the images are burned from a laptop computer to a DVD. All laptop computers which contain appropriate software to download video recorded information from vehicles are equipped with a file shredding application which shreds each downloaded file upon being activated by the authorized TTC supervisor.

With respect to the images recorded from the subway system, the TTC stated that images are retained in a controlled-access area of any given subway station. Images are retained for a maximum retention period of seven days, and then overwritten.

In light of the information provided by the TTC, I am satisfied that the destruction methods for images retained from video surveillance cameras are appropriate and in compliance with the requirements under our *Guidelines*. I am also satisfied that

46 See *Guidelines*, page 9.

these destruction methods constitute "reasonable measures" to protect the security of recorded images under section 3 of Regulation 823.

Conclusion: The TTC has proper destruction processes in place for recorded information that is no longer in use.

Issue G: Does the TTC have proper retention periods in place for personal information that is collected?

Section 5 of Regulation 823 establishes a minimum retention period for personal information that has been collected by an institution, and states:

> Personal information that has been used by an institution shall be retained by the institution for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, unless the individual to whom the information relates consents to its earlier disposal.

This provision establishes a minimum one-year retention period for personal information that has been "used." The purpose of this provision is to require that institutions maintain records containing personal information for at least one year in order to facilitate a right of access by individuals to their own personal information.

I note that the one-year retention requirements for records that have been used are not currently expressed in the Policy or in materials provided to my office. Accordingly, I will be recommending that the TTC incorporate the appropriate retention periods into the Policy before it is finalized.

The *Guidelines* elaborate on the retention requirement in the Regulation and recommend a retention period for video surveillance images that have been collected but have not been used, and state:

- The organization should develop written policies on the use and retention of recorded information that:

  …

  – 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.[47]

  …

47 See *Guidelines*, page 8.

In the Policy, the TTC has not finalized the retention period for recorded images collected from video surveillance cameras. However, in materials provided to my office, and addressed above, the TTC has stated that images recorded from surface vehicles would be overwritten after 15 hours if the image had not been used as part of an investigation. For the subway system, images will be overwritten after a period of seven days, if not used.

The TTC has provided my office with Transport Canada's *Closed Circuit Television Reference Manual for Security Applications,* which recommends retention periods of between seven and 30 days for images recorded from video surveillance cameras. My office's *Guidelines* recommend a shorter retention period of 72 hours. Video surveillance cameras operated by the Police in the entertainment district of downtown Toronto currently operate successfully with a maximum retention period of 72 hours and have operated on this basis for several years. In my view, 72 hours provides a sufficient window of time for the TTC and the Police to determine if an incident has occurred and if video surveillance footage may be relevant to its investigation. Therefore, I see no reason to extend the retention period beyond the recommended 72 hours.

Conclusion: The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.

Issue H: Has the TTC undertaken all appropriate steps prior to implementing video surveillance?

With respect to Privacy International's assertion that the "scheme is being deployed without consideration of privacy and associated protocols," I note that the TTC's draft Policy has actually been modelled on the recommended provisions outlined in my office's *Guidelines for the Use of Video Surveillance Cameras in Public Places*, which are intended to provide direction on the deployment of video surveillance in a privacy-protective manner. The TTC has been careful to ensure that the key privacy provisions of the *Guidelines* have been incorporated into their draft Policy.

Our *Guidelines* provide recommendations regarding the steps that institutions should take prior to engaging in video surveillance.

The *Guidelines* state, in part:

- An assessment of privacy implications should be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated by examining the collection, use, disclosure and retention of personal information.

…

- 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.[48]

…

As discussed above, the TTC has engaged in public consultation on certain elements of its video surveillance system. For instance, the TTC has sought the public's opinion on the design of new streetcars, and invited the public to provide comment on mock-ups of the new subway cars. In both cases, the presence of video surveillance cameras was considered to be positive by those involved in the consultation process.

With respect to the requirement that the TTC conduct a formal assessment into privacy impacts, the TTC noted that, as an Appendix, the Policy contains a *Surveillance Video Security Threat Assessment*. The TTC noted that a formal threat assessment will be completed prior to the finalization of its Policy, which is planned for early 2008.

The IPC *Guidelines* recommend "extensive" public consultation to ensure that stakeholders are educated and informed of the video surveillance system and given an opportunity to provide feedback. While the TTC has undertaken some consultations, these consultations were not specific to the TTC's overall video surveillance program. I am not convinced that these consultations fulfill the requirements of our *Guidelines* and have concluded that the steps taken prior to the implementation of video surveillance by the TTC, specifically with respect to extensive public consultation, are not sufficient.

As the TTC continues to expand its video surveillance program, I recommend that more public consultations take place, possibly in the form of town hall meetings, to broadly educate the public and publicize the expansion of the video surveillance system in Toronto's public transit system. In addition to conducting public consultations, I recommend that the TTC inform the public of its video surveillance program by publishing general information on its website and in printed materials, as appropriate.

Conclusion: As the TTC expands the use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

Issue I: Is the TTC's video surveillance system subject to regular audits?

In the context of video surveillance, an audit should be viewed as a thorough examination of an institution's policies, practices and procedures, as well as a test of internal compliance with the obligations set out under these documents. The audit requirement is expressed in our *Guidelines* as follows:

48 See *Guidelines*, page 4.

> Organizations should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the organization'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.[49]

The general utility of organizational privacy audits has been recognized by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA), who have jointly published their *Generally Accepted Privacy Principles (GAPP) – A Global Privacy Framework (the GAPP Privacy Framework)*.[50] The *GAPP Privacy Framework* was developed to assist organizations in identifying and managing privacy risks and serves as an excellent basis for conducting independent audits.

The TTC has developed comprehensive policies and procedures that seek to minimize improper access and intrusions into the privacy of individuals. The systems described above, which contemplate defined staff privileges and a paper trail of access documented through logs, are also intended to prevent potential abuses of their surveillance system.

Notwithstanding these protections, the size and complexity of the TTC as an organization, as well as the extent of surveillance due to the number of cameras in operation, gives rise to the potential for abuse. Accordingly, regular system-wide audits (at least on an annual basis) will help to ensure that the system is operating properly with respect to privacy and will help to reduce the risk of a privacy breach.

In the materials provided to the IPC, the TTC made reference to plans for conducting annual audits of their surveillance system. In the Policy, under the section "Roles and Responsibilities," the General Secretary of the TTC is listed as being responsible for ensuring Policy compliance and for coordinating annual audits of the TTC's video surveillance system.

The TTC's Policy provides no further elaboration of these audits. There is no separate heading for audits in the Policy nor is there any reference to the requirement that audits be conducted on an annual basis.

Accordingly, I am recommending that the TTC amend its Policy in order to make the audit requirement more explicit. I am also recommending that the TTC provide

49 See *Guidelines*, page 10.

50 The *GAPP Framework* is available from the CICA's website: **http://www.cica.ca/index.cfm/ci_id/36529/la_id/1**

a copy of its first annual audit to the IPC's Policy Department for review. Review by my office will help to ensure that the audit is methodologically sound and comprehensive in its scope. In addition, the initial audit should be performed by an independent third party using the *GAPP Privacy Framework* and should also assess the TTC's compliance with the recommendations made in this Report. This will allow my office to follow up on any shortcomings identified through the audit.

Conclusion: The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the *GAPP Privacy Framework*.

Summary of Conclusions

In summary, I have made the following conclusions in this investigation:

A The information collected by the TTC's video surveillance cameras qualifies as "personal information" as defined under section 2(1) of the *Act*.

B The collection of personal information by the TTC's video surveillance cameras is in compliance with section 28(2) of the *Act*.

C The Notice of Collection is provided to TTC passengers in compliance with section 29(2) of the *Act*.

D The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the *Act*.

E The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

F The TTC has proper destruction processes in place for recorded information that is no longer in use.

G The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.

H As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

I The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the *GAPP Privacy Framework*.

Recommendations

In light of the conclusions contained in this Report, I recommend that the TTC take the following steps to enhance the protection of personal information collected through its video surveillance system. Specifically, I make the following recommendations:

1 That, prior to providing the Police with direct remote access to the video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures be subjected to regular audits, conducted on behalf of the TTC. A copy of the revised draft MOU should be provided to my office prior to signing.

2 That the TTC amend its Policy to reflect the conditions set out in the revised MOU.

3 That the TTC amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

4 That the TTC advise my office of its progress in installing the signs providing Notice of Collection to passengers.

5 That the TTC amend its retention periods for video surveillance images from a maximum of seven days to a maximum of 72 hours.

6 That the TTC amend its Policy to include applicable retention periods, both for when images are used (minimum of one year) and when the images are not used (either 15 hours or 72 hours, depending on where the camera is situated).

7 As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

8 That the TTC include an additional heading in its Policy specifically addressing the annual audit requirement. The Policy should state that the annual audit must be thorough, comprehensive, and must test all program areas of the TTC employing video surveillance to ensure compliance with the Policy and the written procedures. The initial audit should be conducted by an independent third party, using the *GAPP Privacy Framework*, and should include an assessment of the extent to which the TTC has complied with the recommendations made in this Report.

9 That the TTC provide my office with a copy its first annual audit for review, and comment on the details and methodology of the audit.

10 That the TTC provide my office with a copy of its revised Policy no later than one month after the date of this Report.

11 That the TTC should keep abreast of research on emerging privacy-enhancing technologies and adopt these technologies, whenever possible.

12 That the TTC should select a location to evaluate the privacy-enhancing video surveillance technology developed by the University of Toronto researchers K. Martin and K. Plataniotis.

13 Within three months of the date of this Report, the TTC should provide my office with proof of compliance or an update on the status of its compliance with each of these recommendations.

Commissioner's Message

The area of video surveillance presents a difficult subject matter for privacy officials to grapple with impartially because, on its face, it is inherently privacy-invasive, due to the potential for data capture. Despite that fact, there are legitimate uses for video surveillance, as outlined in this Report, that render it in compliance with our privacy laws. The challenge we thus face is to rein in, as tightly as possible, any potential for the unauthorized deployment of the system. We have attempted to do this by ensuring that strong controls are in place with respect to its governance (policy/procedures), oversight (independent audit, reportable to my office) and, the most promising long-term measure, the introduction of innovative privacy-enhancing technologies to effectively eliminate unauthorized access or use of any personal information obtained.

In light of the growth of surveillance technologies, not to mention the proliferation of biometrics and sensoring devices, the future of privacy may well lie in ensuring that the necessary protections are built right into their design. "Privacy by design" may be our ultimate protection in the future, promising a positive-sum paradigm instead of the unlikely obliteration of a given technology. My goal is to have privacy embedded into the architecture of all future technologies, thereby preserving it well into the future.

Ann Cavoukian, Ph.D.
Commissioner