INVESTIGATION REPORT

INVESTIGATION P98-012

Video surveillance by public bodies: a discussion

March 31, 1998

David H. Flaherty
Information and Privacy Commissioner
for British Columbia
4th floor, 1675 Douglas Street
Victoria, British Columbia V8V 1X4
tel. (250) 387-5629
fax. (250) 387-1696
Web site: http://www.oipc.bc.ca

Table of Contents

Executive Summary

This Investigation Report is the result of site visits to public bodies throughout the Province, including the Vancouver Public Library, the headquarters of the Insurance Corporation of British Columbia, and several correctional institutions, police departments, and hospitals. All of these public bodies use video surveillance systems.

I have approached this investigation with the belief that video surveillance technology is neither inherently bad nor good, but that there is both good and bad surveillance. This reflects my practice of acting as a "privacy pragmatist" when addressing privacy problems. However, it has become clear to me during the course of my investigation that, too often, decisions to install video surveillance equipment are made on the basis of the superficial appeal of a technological "quick fix" to a particular problem and are not based on a balancing of the costs and benefits of its use. The pervasiveness of this mentality and its creeping, adverse consequences for personal privacy reduce a privacy advocate's enthusiasm for the type of pragmatism noted above.[1]

One of the key issues in privacy protection is the prevention of unnecessary surveillance of individuals by regulating the collection of personal information. The imperatives of modern technology often aggravate this process.[2] However, the danger lies not in the *technology* but the tendency to consider it as the solution.

The trend is to use video surveillance as a cure-all in the name of public safety and crime prevention. Although these are real issues that require solutions, public bodies must balance such needs against the right of the individual to be left alone. As video surveillance becomes more accessible and pervasive, the need for guidance for all public bodies becomes more pressing. This Investigation Report is written with this requirement to balance competing interests in mind.

This Investigation Report offers guidelines to protect the privacy of individuals and their personal information when video surveillance systems are in use. These guidelines discuss such

matters as the need for written policy, camera locations, times of operation, security and retention of videotapes, public awareness of cameras, control and operation of cameras, audits, use of personal information on the videotapes, and access to personal information on the videotapes.

PART I: The issues and statutory mandate

A. INTRODUCTION

We can only be sure of being free from surveillance today if we retire to our basements, cloak our windows, turn out the lights and remain absolutely quiet. - Gerard La Forest, former Justice of the Supreme Court of Canada.[3]

Physical surveillance is nothing new to society. Yet, with the emergence of increasingly innovative and advanced technologies, modern surveillance has taken on a whole new character. Video surveillance has expanded beyond national security and law enforcement to include public and private sector employers, commercial enterprises and service providers. It is no longer labour-intensive, cumbersome and costly, nor is it primitive. Surveillance technologies now have the ability to penetrate walls, function in the dark, and operate from great distances with such effectiveness that even Mr. Justice La Forest's precautions would offer only a semblance of protection to the most prying of "eyes."

Information obtained through these surveillance techniques can be blended with other sources of information and manipulated with ease. Computerized facial recognition systems already in use in Great Britain and the State of Massachusetts can digitize images from video and search for matches amongst databases of millions of stored faces. Here in British Columbia such a database of digital images already exists in the form of the Motor Vehicle Branch Drivers' Photo Identification Database (DPID).

The use of video cameras for surveillance purposes occurs in both the private and public sectors. Closed-circuit television (CCTV) systems are in use in retail stores, financial institutions, parking lots, and transit facilities, as well as on public highways and in the workplace. However, for the purposes of this investigation, I am only concerned with video surveillance as it is conducted by public bodies in areas within their control. In British Columbia, "public bodies" under the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the *Act*) include the provincial ministries, Crown corporations, agencies, boards, municipal governments, municipal police departments, colleges, universities, hospitals, and the self-governing professions. As the Information and Privacy Commissioner of British Columbia, I have jurisdiction to review the collection of personal information by these public bodies, including by way of video surveillance.

This Investigation Report is the result of various site visits to public bodies that have implemented or plan to implement video surveillance technology for reasons of crime prevention, public safety, or as part of their operational duties. As the enabling technology of

video surveillance becomes more pervasive and accepted, the need for a set of common policy guidelines, and a frank discussion of the balance we seek to achieve among competing values, becomes ever more pressing.[4]

B. STATUTORY MANDATE

Section 3(1) defines the scope of the *Act* to include all records in the custody or under the control of a public body. Schedule 1 of the *Act* defines a record to include "books, documents, maps, drawings, photographs, letters, vouchers, papers and other things on which information is recorded or stored by graphic, electronic, mechanical or other means...." This means that "record" includes videotapes. Section 42(1)(a) is the investigative authority for this Investigation Report:

42(1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may

(a) conduct investigations and audits to ensure compliance with any provision of this Act,
....

Section 26 of the *Act* sets out three conditions under which public bodies may collect personal information: by or under legislation; for a law enforcement purpose; or where the personal information relates directly to and is necessary for an operating program or activity of the public body. If a public body does not have justification for video surveillance by or under legislation, or for a law enforcement purpose, then it must demonstrate why the video surveillance is necessary for an operating program or activity of the public body. This Investigation Report examines the reasons given by two public bodies why video surveillance is necessary for their operating programs. See Part II.D. of this Investigation Report for further discussion of section 26.

C. VIDEO SURVEILLANCE: THE PRIVACY THREAT

In many of its applications video surveillance is widely accepted as useful and even necessary. There is no shortage of supporters. The industry is large and powerful, and the technology itself is attractive to many -- seeming to pose simple solutions to what are often complex problems. However, it is not my business as a privacy advocate to articulate the reasons for the use of such technology.

One of the most disturbing aspects of video surveillance is the almost total absence of public debate on the subject. Simon Davies, one of the founders of the privacy rights organization *Privacy International* and author of the book Big Brother: Britain's Web of Surveillance, noted that surveillance "has the potential to desensitize the population to other, less visible, forms of

surveillance. The ready acceptance of video surveillance might be indicative of the creed `nothing to hide, nothing to fear.' And a nation which happily accepts visual surveillance without debate may easily and happily accept a range of other forms of surveillance, from wire-tapping to identity cards."[5]

I recently commented on the use of surveillance in society:

... my experience in British Columbia is that the pressures for surveillance are almost irresistible for an office such as mine. The bureaucrats and the legislature are under intense pressures to reduce costs, to promote efficiency, and to spend public money wisely. Surveillance technology appears to be a neutral, objective process that must be wielded as a weapon, or at least a tool, against welfare cheats (targeting all those on income assistance), sex offenders (targeting all those who work with children through criminal-record checks), and photo radar (monitoring all cars and photographing the license plates of speeders).[6]

Serious thought needs to be given to the real value of video surveillance. Public bodies should demonstrate its effectiveness for crime prevention or public safety and weigh it against the costs to individual privacy and freedom before they decide to implement surveillance. In other words, the first questions to be answered when speaking to these issues are whether and why, not how.[7] David Boyd of the U.S. National Institute of Justice states it even more succinctly: "This is technology that cuts both ways. It can provide lots of security for people, lots of peace of mind. But at the same time, in the wrong hands, it can be badly abused."[8]

D. THE EXPANSION AND EFFECTS OF VIDEO SURVEILLANCE

In the past decade, the use of CCTV for surveillance and crime control has grown to unprecedented levels. In Britain between 150 and 300 million pounds Sterling (C$348 to 696 million) per year is now spent on surveillance, involving an estimated 300,000 cameras covering shopping areas, housing estates, parking lots and public facilities in many towns and cities.[9] While Britain is the lead nation in implementing CCTV, other countries, including our own, are not far behind. Canada, the United States, Australia and some European countries, which a few years ago might have rejected the technology, are installing cameras at a rapid pace. Already, the cities of Sherbrooke and Hull, Quebec, have installed cameras in their respective downtown cores in an effort to reduce crime.

Goderich, Ontario, a small resort community on the shores of Lake Huron, studied a plan to install video cameras around its courthouse and public square. The community eventually found the cost of such a system prohibitive, but it is likely only a matter of time before other communities find themselves looking into the eye of the camera.[10] In Suisun City, California, local authorities are installing cameras to combat gang activity spilling over from nearby Oakland and San Francisco -- boasting that no one coming into Suisun goes unnoticed.[11] From urban centres such as Miami's Dade County to British Columbia's remote Chilcotin region, school administrators are turning to CCTVs in buses, hallways and even in playgrounds in an effort to check unwanted behaviours, from bullying to rowdiness.[12]

This last statement demonstrates what Nigel Waters, former head of the Privacy Branch of the Australian Human Rights and Equal Opportunity Commission, describes as the arguably more sinister aspect of technology expansion. "Function creep" is the well-intentioned extension of the original purpose of video surveillance into a broader public order role, and the use of the camera as an instrument of social control.[13] Simon Davies notes that while camera systems were originally installed to deter burglary, assault, and car theft, most camera systems actually have been used to control public order and combat "anti-social behaviour," including many such minor offenses as littering, urinating in public, traffic violations, obstruction, drunkenness, and evading meters in town parking.[14] What is apparent and indeed disturbing is that in the "absence of a wide ranging public debate...the packaging and marketing of CCTV has been instrumental in the shaping of favourable public opinion."[15] Industry is driving CCTV and it is changing from an integral part of crime prevention policy to an integral element in the construction of a disciplinary society in the "Foucauldian sense."[16] Bruce Phillips, Privacy Commissioner of Canada, has stated: "We must accept that [video surveillance] is here to stay, and [is] going to multiply. The real issue is whether in the process of embracing all this technology we are going to put in place proper safeguards...."[17]

Another questionable use of CCTV may be for monitoring the performance of staff -- for example, in an attempt to measure their productivity or even inadvertently as part of an unrelated operation (i.e., crime prevention). Most people do not want to work with a camera monitoring them, except in unusual circumstances such as a prison or other locations where threats to their personal safety exist.

Despite massive adoption of such technology, there has been almost no evidence published in the United Kingdom, or other countries, showing that surveillance cameras have had an overall deterrent effect. In fact, surveillance may only serve to *displace* crime. Richard Thomas, Acting Deputy Chief Constable for Gwent, U.K., recently told the BBC that he believed video surveillance simply pushed some crime beyond the range of the cameras.[18] In an interview with ABC News' 20/20 investigative program, Leslie Sharp, Chief Constable for Scotland's Strathclyde Police Department, said, "I don't believe that just because you've got cameras in a city center that everyone says `Oh well, we're going to give up crime and get a job.'"[19]

Programs elsewhere have had mixed results. Dave Banisar, of the Electronic Privacy Information Center in Washington D.C., has pointed out that CCTV failed to deter crime in Times Square when put to the test by New York City. When officials in New Jersey installed cameras in subway stations, crimes actually increased.[20]

In fact, it is difficult to determine how much crime surveillance deters because, obviously, crimes that have not happened cannot be measured directly. Testing this effect requires detailed monitoring and analysis of crime statistics. To date, no such proper, detailed, independent study has been undertaken in this or other countries. Another U.K. Home Office report notes: "Very few evaluations of town centre schemes have been carried out, and those that have only look at the effect of cameras in the short term."[21] A 1996 South Bank University study stated: "CCTV has recently been the subject of several television documentaries and...banner headlines claiming large reductions in recorded crime. In the main, these claims are not based on any substantial research."[22] "In a report to the Scottish office on the impact of CCTV, Jason Ditton, Director

of the Scottish Centre for Criminology, argued that the claims of crime reduction are little more than fantasy. `All (evaluations and statistics) we have seen so far are wholly unreliable.' The British Journal of Criminology went further by describing the statistics as `...post hoc shoestring efforts by the untrained and self interested practitioner.'"[23]

E. PRIVACY, CIVIL LIBERTIES AND SOCIAL CONSEQUENCES

While most people have an instinctive aversion to being watched, the "chilling effect" of video surveillance on public behaviour is difficult to determine.[24] One thing is clear: issues raised by the video surveillance debate go far beyond arguments of its crime-fighting efficacy. Video surveillance in public places is as much a civil liberties issue as it is a privacy issue, and those civil liberties concerns are closely related to other prized community values, including freedom of assembly and movement.[25]

Nigel Waters points out that video surveillance, unlike more traditional forms of surveillance, is random and indiscriminate in its gaze. Video surveillance involves the collection of personal information without the consent of those under surveillance:

Everyone coming into view -- shoppers, children, lovers, and the socially disadvantaged -- is captured by the cameras recording the movements of daily life without regard to whether a crime is being or is likely to be committed and with no grounds for suspicion because most cameras cannot be made simply to record particular incidents or serious crimes. Everyone suffers the infringement of their privacy and of the right to go about their daily lives free from surveillance.[26]

The above is especially true when images are recorded on tape (the practice for most public bodies in British Columbia). "What it does...is both frightening and, I think, humiliating to a society that feels it has to monitor the every movement of its fellow members," said Robert Ellis Smith, privacy advocate and publisher of the Privacy Journal. According to Smith, "it has created a society that relies too much on technology and not enough on trust."[27]

The non-discriminatory nature of video surveillance is commonly cited as the most worrisome aspect of this kind of technology. This is a function of the technology itself and not of its use. CCTV systems are not inherently evil; rather, the real danger lies in the tendency for a public body to allow the system to be the solution.

A number of authors have recently analyzed the effects of CCTV in generating this novel and unique form of passive discrimination. The technology segments public space in a way that anonymously assigns social status on the basis of a person's appearance or other criteria of "undesirability." These authors argue that video surveillance alters individuals' relationships with public space and public authority and increases the chance that instantaneous and arbitrary decisions about guilt or innocence will be made on illegitimate grounds. This is an important equity issue, in which marginalized and socially disadvantaged groups, who already receive disproportionate attention from the state, are more likely to come to notice because of their

unusual or stereotyped appearance or behaviour. The outcome is not just a change in relations between the state and those citizens, but also a change in nature of public space for all.[28]

A concrete example of the way video surveillance disrupts public space and reorganizes the relationship between individuals and public authority arises in the case of media "ride-along crews" who accompany police officers on patrol. In Investigation Report P95-004, I commented on their potentially adverse impact:
In my role as Information and Privacy Commissioner, it is essential, where public bodies are involved, to encourage them to strike the appropriate balance between the right of access to information that is of public interest and the protection of an individual's right to be left alone.

In the case of police `reality television' shows, the public's right to know about the daily operations of its local police department competes with the right to privacy of the individuals in contact with police. These individuals may not yet have been charged with an offence, let alone convicted, when their faces are broadcast on television for an entire community to see. Thus, for the individual, the possibility of a mistaken identity, a withdrawn complaint, an unfortunate moment, or one of the simple misunderstandings that are a part of everyday life loom large as a serious threat to the privacy rights of each person.[29]

These same concerns apply to the use of video surveillance by public bodies.

There are conflicting opinions within the police community on the use of video surveillance. Referring to his force's mania for CCTV, one British police officer told ABC News' 20/20 program, "We will gradually drive the criminals further and further away, and eventually I hope to drive them into the sea."[30] Contrast this with the Amsterdam police, who, although they planned to install their own cameras in high-crime areas throughout the city in the fall of 1997, still believe that camera surveillance is getting out of hand. "We're absolutely against putting cameras all over the place," says police spokesman Klaas Wilting. "We feel that people have a basic right to privacy."[31]

In the information society, tension will arise between the dignity and autonomy of the individual -- that is, one's ability to control the collection and dissemination of information about oneself -- and the requirement for personal information which organizations and other individuals may require to fight crime, to provide services, or to enter into other kinds of relationships. A certain level of knowledge, different for each type of relationship, is required in order to determine whether or not the parties can trust each other. It is important for public bodies to remember that this is a two-way street. If a public body requires personal information about a client or member of the public in the form of video recording, the public body must also inform him or her why the public body needs this information, for what purpose it will use the information and for how] long it will retain the information. This exchange is fundamental to establishing trust, something which, as we see in the next section, is somewhat lacking.

F. PUBLIC PERCEPTIONS OF VIDEO SURVEILLANCE

The general public is becoming increasingly concerned about the use of video surveillance for the collection of personal information. A 1991 survey of employees throughout the United States revealed that 62 percent disagreed with the use of video surveillance (including 38 percent who "strongly disagreed").[32] In 1994, an Equifax Canada privacy survey discovered that 43 percent of the public believes that "technology has almost gotten out of control." The same survey showed that there has been an incremental increase in the concern about, and the level of importance attached to, privacy issues among Canadians.[33]

In 1992, a U.K. Home Office survey highlighted the extent of concern. The survey found that thirty-six percent of the respondents did not agree with the proposition that "the more of these cameras we have, the better."
...fifty per cent of people felt neither government nor private security firms should be allowed to make decisions to allow the installation of CCTV in public places. Seventy-two per cent agreed `these cameras could easily be abused and used by the wrong people.' Thirty-nine per cent felt that people who are in control of these systems could not be `completely trusted to use them only for the public good.' Thirty-seven per cent felt that `in the future, cameras will be used by the government to control people.' While this response could be interpreted a number of ways, it goes to the heart of the privacy and civil rights dilemma. More than one respondent in ten believed that CCTV cameras should be banned.[34]

G. CASE STUDIES

Under section 42 of the *Act*, I have the power to audit the information-handling practices and procedures of the over 2,000 public bodies under my jurisdiction. I have continued to emphasize this aspect of my mandate as a primary means of raising the consciousness of public bodies about the importance of fair information practices. These practices as they relate to this particular topic are set out in Part 3 of the *Act*, and regulate how a public body may collect, use, and disclose personal information as part of its operations.

The following case studies illustrate the variety of ways that video surveillance is used in real-world settings in British Columbia. They show how the uses for information have increased beyond what formerly occurred when records were produced and stored in paper form only. A wide range of public bodies now use video surveillance systems, including police departments, hospitals, schools, liquor stores, and corrections facilities.

Vancouver Public Library, Main Branch

In response to a history of crime prevention and public safety issues documented over many years of operation at its previous location at 750 Burrard Street, the Vancouver Public Library decided to install a video surveillance system in its new downtown main branch complex, completed in early 1995. The nine-floor building, seven of which are occupied by the Library, receives an average of 6,300 daily patrons and is a high-traffic public space.[35]

Although over thirty CCTV cameras were installed, administrators have primarily restricted them to off-limits zones such as fire escapes and support areas separate from public access. One exception is the camera observing all patrons entering and leaving the main entrance; another is the camera focused on the entrance to locked children's washrooms in the children's reading area -- an area which historically has received unwelcome attention from adult predators, including pedophiles.

Since the goal of the new CCTV system was to ensure public safety and prevent vandalism, the Library states that it developed a strategy to achieve these goals without infringing on the rights of the visiting patrons or altering the spirit of community that libraries represent. Rather than blanketing the entire Library with cameras, an invasive method, the Library has placed the CCTV cameras to cover major access points and problem areas that it has identified.

My office conducted two site visits to the Library. Based on these visits and discussions with Library staff, I am satisfied that the video surveillance system incorporates some of the benchmark fair information principles that are the heart of every privacy protection code. By this I mean that the Library has taken some steps to minimize its collection of personal information by means of CCTV. Most of the cameras are not in public areas or have been installed to monitor and assist patrons to leave the building during an emergency.

The Library's security staff have informed my office that the cameras have been used in the arrest and conviction of six vandals or thieves to date, and used to identify and arrest suspects in other cases which are pending legal resolution. They estimate that without the deterrent factor of the cameras, the level of criminal activity at the Library would be 50 to 100 percent higher.[36]

Despite these claims of success, the Library's video surveillance system has problems which need to be addressed. The first issue that my office identified was what is in effect, if not in intent, the hidden camera at the main entrance recording all persons entering or exiting the Library. When questioned, security personnel informed us that the Library has had thefts of computers and books by people who have simply walked or run out the main gate; the purpose of this camera was to prevent such incidents. The camera in the main entry lobby also led to the arrest of a suspect for assault on a security guard.

Although the installation at the entrance was done with good intentions, the hidden camera does not act as a deterrent. The question arose in discussion of why a *hidden* camera? If the purpose is *deterrence*, then a visible camera and well-marked notification signs might serve much more effectively. A dummy camera and signs could have the same deterrent effect. Further, if statistics show that there is a problem of theft and vandalism of either books or fixed assets through the main entrance, then the Administration should look at other methods of addressing this problem first. It was pointed out by the Library security staff that there had been a problem with people simply jumping the entrance gate. As the gate is quite low, it is not difficult to imagine such a scenario. However, it is unlikely that a covert camera would deter those brazen enough to attempt the effort in the first place. This is a good example of using CCTV as a "simple solution" to a complex problem without consideration of the potential for unintended consequences.

The Library states that it did not intend the camera at the entrance to be a covert or hidden camera. Its primary concern is to document individuals leaving the building to assist in stemming the significant losses by theft that the Library is experiencing. The camera also records interactions between security guards and library patrons at the main entrance. The videotape is not used for other purposes and is retained for a limited time.

A second issue was that the Library did not provide sufficient notification that patrons might be under surveillance upon entering the Library. A few signs were put up at the entrance after the visits from my office, but the notice is inadequate for this purpose. Such signs must be placed in prominent, visible locations to notify patrons that they will be monitored in this public space. The Vancouver Public Library intends to do so, which, in my judgment, will enhance the deterrent effect of such video surveillance.

A third issue is that the Vancouver Public Library does not have a written policy governing the use of its video surveillance system. Without a policy to govern a surveillance system's use and purpose, it is difficult for a public body to comply with the fair information principles of use, disclosure, or retention of personal information. Who decides how long recorded tapes are kept? Who can view them and for what purpose? Can they be used to make a promotional television commercial for the Library? Can they be aired by a local television station as part of a story?

A clear, concise policy will help ensure fair and consistent treatment of personal information collected by public bodies. The Vancouver Public Library intends to develop a written policy with guidance from this office.

Insurance Corporation of British Columbia

The Insurance Corporation of British Columbia (ICBC) is the primary provider of automobile insurance in the Province. The purpose of a site visit to ICBC headquarters was to collect data on the placement and use of over sixteen CCTV cameras and associated monitoring systems in and around the main ICBC facility, and to consult on any similar installations and practices in regional claim centres across the Province.

The ICBC video surveillance system at the main headquarters in North Vancouver consists of covert cameras monitoring the two reception desks at each of the main entrances and pan-and-tilt and "regular" CCTV cameras on the outside of the complex. Of the regular CCTV cameras, eight of these locations have motion detectors connected to the cameras. These provide a signal to the monitoring station only when motion is detected in front of the cameras; therefore, the eight cameras are on only during activity periods. Each of the reception desks is staffed by security guards. All visitors must present themselves to a guard, sign a log book, and wait for an ICBC employee to escort them to their destination.

Members of my office were informed that the cameras at the front reception desk were in place to back up the security staff in case of "belligerent clients." There was brief anecdotal discussion of an instance when this did occur but, to the best of our knowledge, no statistics have ever been compiled on the frequency of these incidents. Settling the business of insurance claims can often be a sensitive and painful issue for insurance claimants. While over 82 percent of claims

customers indicate that they are either satisfied or very satisfied with both the service and the settlement they received from ICBC, the remaining 18 percent are not.[37] Troubled or dissatisfied clients may pose safety risks to ICBC employees; these clients are the primary reason ICBC decided to install video surveillance systems in its headquarters in North Vancouver and in claim centres across the Province.

Of particular note at ICBC are pan-and-tilt zoom cameras located on the outside of the main building, which cover external promenades and an adjacent ICBC complex. Cameras of this nature could be used to follow a person's movements and focus on locations outside ICBC's property (e.g., a restaurant patio across the street). As in all cases, public bodies should ensure that cameras only capture activity within the complex or directly related to ICBC facilities.

ICBC officials offer the following explanations and rationales for the use of video surveillance: CCTV cameras also provide a source of information that can be used to protect not only the individual, but the corporation. For example, the camera monitoring the access points may inhibit theft and record what transactions have transpired. Often mail items are left at each of the reception desks, and the camera will confirm if an item was in fact dropped off.

With respect to safety issues, if a building is to be evacuated, the monitoring stations may be used to ensure that individuals have not re-entered the building. As it is impossible for the security guard to be in all locations of the building, the monitoring station is used as an extension of the security guard. In the event of a potentially volatile situation between a security guard and a client, the camera recording can be used to examine the body posture and positioning of the security guard, and how each of these can be adjusted to help eliminate a threat and increase public safety.

As ICBC deals directly with the public, the cameras also provide a realistic look at the activity levels at a variety of locations, and where security personnel or other ICBC representatives should concentrate their efforts. This allows ICBC the ability to organize itself in order to deal with the public more efficiently.

With regard to covert cameras, visible cameras may incite a client who may then pose a risk to ICBC employees and possibly their satisfied clients. The idea of the covert camera is to remove a theatre for a client who wishes to create a scene. The covert camera is a way of having more people placed into the area to increase the level of safety, while maintaining good customer relations. This is the reason that the covert cameras are only used at the public access points at both reception areas.

There is no absolute way to guarantee that all persons entering an ICBC location are aware that they are being monitored; however, due diligence has been taken so that the expectation of privacy cannot be assumed.[38]

It is evident from these statements that ICBC's practice of video surveillance is heavily weighted towards the protection of its interests and what it perceives to be the public interest.

Like the Vancouver Public Library, ICBC does not have a written policy regarding video surveillance cameras. ICBC officials described a public safety mandate for the presence of video cameras; ICBC intends to develop this mandate into policies in the near future with the assistance of my office.

Part II: The *Freedom of Information and Protection of Privacy Act*

A. INTRODUCTION

Part 3 of the *Act* sets out the requirements for protecting the personal information in the custody or under the control of public bodies. These requirements are based on fundamental and internationally-recognized principles of privacy often referred to as "fair information practices":

- that a person's personal information is her or his own;
- that a person has a right of access to her or his personal information; and
- that a person has the right to control her or his personal information and communicate or retain it as she or he sees fit.

The *Act* therefore imposes on public bodies an obligation to protect the personal information in their custody or under their control by limiting collection, use, disclosure and retention. The retention periods for personal information should be as short as possible -- public bodies keep personal information only as long as required by law or by operational need (see section 31 of the *Act*). When the retention period expires, public bodies should destroy personal information using secure disposal methods (e.g., shredding).

The following discussion is designed to guide public bodies through the process of applying the fair information practices to a video surveillance system. Part III of this Investigation Report lists guidelines for developing written policy on the development, deployment and use of a video surveillance system in public bodies. Where public bodies choose to implement video surveillance, these guidelines will assist the public bodies to comply with the requirements of the *Act.*

B. RELIANCE ON VIDEO SURVEILLANCE

Public bodies should only use routine video surveillance when the benefit to the community outweighs, to a substantial degree, other competing social interests and individual rights, especially the preservation of personal privacy. Whenever possible, public bodies should preserve the rights and freedoms of citizens, including the right to be free from unwarranted surveillance by government and law enforcement agencies when visiting public bodies. There are justifiable and legitimate uses for surveillance, such as law enforcement, public safety, and employer interests (e.g., security of clients, employees, and physical assets). Therefore the question is whether a video surveillance system is the necessary or only solution.

Easily the most common error made when a public body is faced with a decision of whether to use new technology, such as video surveillance, is that the primary consideration becomes one of installation and not use. The vendors of such technology are often the driving forces behind these decisions. This is a mistake. As individuals become more aware of their privacy rights, public bodies must be able to demonstrate having fully considered the issues involved in video surveillance.

The arbitrary invasiveness of video surveillance is such that I strongly encourage and would, in some cases, require that public bodies investigate problem-solving measures other than video surveillance. Restricting access to problem areas with pass cards or identification badges, increased lighting, and removing the incentive for vandalism or other undesirable behaviour, are all examples of steps that should be taken before installing video surveillance systems. If no demonstrable benefit is realized, then public bodies may be justified in moving up a "ladder of intrusiveness" to the application of a CCTV system. In cases when a CCTV system has already been installed, the ladder of intrusiveness still applies. Public bodies can operate video surveillance systems in any of the following increasingly-intrusive ways and remain effective:

a) cameras and public notification signs are in place, but cameras are not on or recording;
b) cameras and public notification signs are in place, but cameras are used for monitoring and not recording to tape;
c) cameras and public notification signs are in place, but cameras are on for monitoring and only those in high-incidence areas are recording; or,
d) cameras and public notification signs are in place, but cameras are on only during high-incident or high-risk time periods. Alternatively, cameras can be switched on randomly.

C. THE IMPORTANCE OF WRITTEN POLICY AND NOTICE

Principle 2 of the 1996 *Canadian Standards Association Model Code for the Protection of Personal Information* (the *CSA Code*) states that the purposes for which personal information is collected shall be identified by the organization *at* or *before* the time the information is collected.[39] Although the *CSA Code* was designed as a certified standard for the private sector and is not binding on public bodies, the *CSA Code* is a useful tool in addition to the *Act* for any organization that collects personal information. Principle 2 emphasizes the importance of written policy for video surveillance systems.

Consider the following situation. An applicant requests a copy of a surveillance videotape which may have captured a purse-snatching incident on the premises of the public body. Unfortunately for the applicant, the public body already has routinely erased the surveillance videotape because the retention period has expired. Without a written policy describing the retention and disposal of records, the applicant could argue that the videotape had been destroyed precisely *because* he or she asked for it and there would be little the public body could say to prove otherwise.

Written policies governing the use of video surveillance systems protect both public bodies and applicants who request access to video surveillance records: public bodies know when to dispose

of video records; applicants know when they can request records. This raises another consideration: if a public body *creates* a record, then it must be prepared to disclose that record under the freedom of information process if it is requested. In other words, creating a record in the first place will often mean increased and unwanted exposure at the expense of the public body.

D. *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*: PART 3

Purpose for which personal information may be collected -- section 26

Section 26 of the *Act* recognizes a public body's need to collect personal information in order to carry out its mandate and to provide services, but restricts that collection to a defined set of circumstances. Section 26 also acknowledges that public bodies which engage in law enforcement activities need more flexibility in the scope of their collection of personal information.[40] When a public body considers implementing a video surveillance system, it should review the requirements of section 26. Is the surveillance expressly authorized by legislation? Is the surveillance conducted for law enforcement purposes? Is the surveillance directly related to and necessary for an operating program or activity? If the answer to these questions is "no," then the surveillance is likely not justified.

Section 26 of the *Act* reads as follows:

26. No personal information may be collected by or for a public body unless:

> a) the collection of that information is expressly authorized by or under an Act*,
>
> b) that information is collected for the purposes of law enforcement, or
>
> c) that information relates directly to and is necessary for an operating program or activity of the public body.

** Note: the legislation in question may expressly authorize the collection of personal information. Usually, however, the legislation will only give authority for a particular program, with only implied authority for the collection of personal information.*

How personal information is to be collected -- section 27

Section 27(2) requires public bodies to notify the person from whom the information is collected of the purpose and authority for collection unless the collection relates to the matters set out in subsection 27(3). Thus, the *Act* imposes three conditions: public notification of any video surveillance being conducted by a public body; the purpose for which it is being conducted; and a designated person from whom more information about the program may be obtained. All of these are required unless exempted under subsection 27(3) (see Part III.5 of this Investigation Report, below).

Section 27(2) of the *Act* reads as follows:

27(2) A public body must tell an individual from whom it collects personal information:

a) the purpose for collecting it,

b) the legal authority for collecting it, and

c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

In certain circumstances, personal information can be collected, used, or disclosed without the knowledge and consent of the individual. Legal, medical, or security reasons may make it impossible or impractical to seek consent. For example, when public bodies collect information to detect and prevent fraud, seeking the consent of the individual might defeat the purpose of collecting the information.

Protection of personal information -- section 30

Public bodies must protect personal information by using security safeguards appropriate to the sensitivity of the information. Section 30 requires the head of a public body to provide appropriate physical and procedural security measures to protect personal information in the custody or under the control of the public body.

Public bodies must limit access to CCTV monitor viewing areas to staff with that responsibility, whether to operate the equipment or to view the images. An occurrence book should record staff on duty each shift, and the names of any persons or groups that have been authorized with day to day responsibility for the scheme. If public bodies leave CCTV monitors unattended, the area in which they are kept should be secured against unauthorized entry.

Public bodies should create policy governing the use of and access to recorded material, based on these guidelines:

- recorded material will be used only for purposes defined in this code of practice;
- recorded material will not be sold or used for commercial purposes or entertainment;
- access to recorded material will only take place as defined in the code of practice;
- the display of recorded material to the public will only be allowed in accordance with the law (e.g., police investigations of crimes or in any other circumstances provided by law).

<u>Use of tapes</u>

- public bodies should use tapes in rotation and should keep the tapes for no longer than the operational requirements of the public body;
- public bodies must erase all previous recordings on the tapes prior to reuse. This practice will ensure that the integrity of the process is maintained consistently throughout;

- public bodies will securely dispose of old tapes. Physically breaking open a videotape cassette is not sufficient: the tape should be shredded, burned or degaussed (magnetically erased).

Section 30 of the *Act* states:

30. The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Retention of personal information -- section 31

Principle 5 of the *CSA Model Code for the Protection of Personal Information* stresses the importance of *minimizing* retention. It reads "personal information [should] be retained only as long as necessary for the fulfillment of [the] purposes [for which it was collected]."[41] The *Act* is silent on how long this retention period should be, subject to section 31, and retention will vary depending on the uses made of the video surveillance record. The exception to this rule is if the video record is used to make a decision directly affecting that individual, in which case the record must be retained for at least one year after that decision is made.

Section 31 of the *Act* states:

31. If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

Public bodies that are governed by the *Document Disposal Act*, R.S.B.C. 1996, c. 99, should ensure that their records retention and disposal schedules include a retention period for surveillance videotapes, where applicable.

Use of personal information -- section 32

Section 32 of the *Act* requires public bodies to use personal information only for the reasons for which it was originally collected, with three exceptions. These exceptions are given below. Similarly, Principle 5 of the *CSA Code* states that personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law.[42]

Section 32 of the *Act* states:

32. A public body may use personal information only:

> a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
>
> b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

Part III: Video Surveillance Privacy Guidelines

Public bodies should review these guidelines before considering the use of video surveillance:

1. Written Policy

- Public bodies that use video surveillance equipment should develop formal written policy to govern the use of the equipment.
- Public bodies should give this policy to employees and contractors so that they can review and apply it to their duties and functions.
- Public bodies should incorporate the video surveillance privacy guidelines into staff training and orientation programs.
- Public bodies should provide the policy to the public upon request.

The following points are issues which public bodies should address when drafting this policy.

2. Camera Location, Operation and Control

- Public bodies should carefully chose sites for camera installation such that their placement is restricted to identified public areas.
- Areas chosen for surveillance should be where surveillance is a necessary and viable deterrent.
- Cameras should not be positioned to monitor areas outside the building or other buildings unless necessary to protect external assets or ensure personal safety.
- Public bodies should not direct surveillance cameras to look through windows to areas outside of the building, unless necessary to protect external assets or ensure personal safety of patrons and employees. Cameras should not be directed to look through the windows of adjacent buildings.
- Cameras should not monitor areas where the public has a reasonable expectation of privacy (e.g., change rooms and adult washrooms).
- Public bodies should be prepared to justify use of surveillance cameras on the basis of quantified reports of incidents of theft, violence, or other breaches of security.
- Only authorized persons so tasked shall have access to the monitor operation controls.

3. Operational Times

- Public bodies must have a degree of flexibility in the approved operation times in recognition of the random nature of the incidence of crime.
- Public bodies should restrict use of video surveillance to identifiable time periods when there is a higher likelihood of crime being committed and detected in the particular vicinity.

4. Protection of Information and Disclosure

Section 30 of the *Act* requires that the head of a public body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Consider the following four problem areas:

a) *Security and retention of tapes*

- Store all tapes not in use securely in a locked receptacle.
- Number and date all tapes that have been used and retained according to camera site.
- The controlling officer must authorize access to the tapes.
- Log all episodes of access to, and use of, recorded material.
- Retain tapes for one year if personal information on the tapes has been used to make a decision that directly affects an individual (see section 31 of the *Act*).
- Retain and store tapes required for evidentiary purposes according to standard procedures until they are requested by law enforcement authorities.
- Complete a tape release form before disclosing tapes to appropriate authorities. The tape release form should indicate who took the tape(s), when this occurred, and if they will be returned or destroyed by the authorities after use.

b) *Disposal and destruction of tapes*

- Public bodies must securely dispose of old tapes. Physically breaking open a videotape cassette is not sufficient: the tape should be shredded, burned or degaussed (magnetically erased).

c) *Video monitors*

- Video monitors should not be located in such a position as would enable public viewing.
- Only the controlling officer or individuals authorized by that officer, or members of the police, should have access to the video monitors while they are in operation.
- Video monitors should be in a controlled access area.

d) *Disclosure*

- Section 33 of the *Act* governs disclosure of personal information by public bodies.
- In addition to section 33, a public body may disclose personal information for a research purpose, including statistical research, *subject to certain criteria* under sections 35 and 36 of the *Act*.

5. Public awareness of cameras

Under section 27(2) of the *Act*, public bodies must notify persons from whom personal information (including video surveillance of identifiable persons) is collected of that collection, the purpose and legal authority for the collection, and provide contact information for the

controlling officer, including title, business address and telephone number. Section 27(3) of the *Act* creates exceptions to this rule where:

> (a) the information is about law enforcement or anything referred to in section 15(1) or (2), or
>
> (b) the minister responsible for this Act excuses a public body from complying with it because doing so would:
>
> > (i) result in the collection of inaccurate information, or
> > (ii) defeat the purpose or prejudice the use for which the information is collected.

- Public bodies should notify the public of camera location(s) at the perimeter of public areas, so that the public has ample warning before entering a monitored area.
- Signs should warn the public that the camera is or may be in operation, which will serve as a general crime deterrent.
- The public body's system should identify the corporate operator of a surveillance system and give an official contact person and address where they can be reached for further information.

6. Audits

- All camera operators must be aware that their camera operations are subject to audit and that they may be called upon to justify their surveillance interest in a member of the public or employee of the public body.
- ***Internal audit:*** public bodies should appoint an internal review officer to audit the use and security of the surveillance cameras, including monitors and tapes. The results of each review should be documented.
- ***External audit:*** the Office of the Information and Privacy Commissioner may conduct periodic audits of public bodies' video surveillance systems under the authority of section 42(1)(a) of the *Act*. These audits will review public bodies' compliance with the guidelines in this Investigation Report.

7. Use of information collected

Recorded videotape is a record under the *Act* and therefore is subject to section 26 which governs collection of personal information. Here are guidelines for the collection of personal information in video surveillance systems:

> a) public bodies may use video surveillance to detect or deter criminal offences which occur in view of the cameras;
>
> b) public bodies may use video surveillance for:

(i) inquiries and proceedings relating to law enforcement;
(ii) research (i.e., the nature of area usage, pedestrian traffic patterns, or evaluation of the operation of particular camera systems);

c) public bodies shall not use video surveillance for other purposes unless expressly authorized by or under an *Act*.

8. Access to personal information

- An individual who is the subject of video surveillance has a right to request access to the tape under section 5 of the *Act*.
- Access in full or in part may be refused on one of the grounds set out in Division 2 of Part 2 of the *Act*. However, if that information can reasonably be severed from a record, an applicant has the right of access to the remainder of the record.

CONCLUSION

I strongly encourage all public bodies that use video surveillance to comply with the recommendations of this Investigation Report. I have found that the use of video surveillance by public bodies is justified only if such information collection is both necessary under section 26 of the *Act* and follows the fair information practices outlined in this Investigation Report. My office will continue to work with the Vancouver Public Library and the Insurance Corporation of British Columbia to ensure that both public bodies adopt and implement the recommendations in Part III of this Investigation Report.

David H. Flaherty
Information and Privacy Commissioner
Victoria, British Columbia
March 31, 1998

ACKNOWLEDGMENTS

I would like to acknowledge the contributions to this Investigation Report of Nigel Waters, a private consultant and former Head of Unit, Privacy Branch, Australian Human Rights and Equal Opportunity Commission; Dr. Colin Bennett of the University of Victoria; Jonathan Bamford, Assistant Registrar of the U.K. Data Protection Registrar's office, Great Britain; C. William Webster, researcher at Glasgow Caledonian University; and Chief Constable John Burrow, Essex, U.K.

Investigation conducted by Jason M. Young, R. Kyle Friesen, David H. Flaherty, and Lorrainne A. Dixon
Investigation report written by Jason M. Young, R. Kyle Friesen, and David H. Flaherty.

Appendix 1: Fair Information Principles from the CSA Model Code for the Protection of Personal Information

These are the ten principles of the *CSA Model Code for the Protection of Personal Information*.

1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8 Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of her or his personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Footnotes

1 See David H. Flaherty, "Risks and Benefits in Personal ID Systems," Transnational Data and Communications Report (November / December 1993).

2 David H. Flaherty, "Nineteen Eighty-Four and After," Government Information Quarterly, Vol. 1 (1984) 431-441.

3 Hon. Sheila Finestone, Chair, Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, Privacy: Where Do We Draw The Line?, April 1997, p. v.

4 David H. Flaherty, "Workplace Surveillance: The Emerging Reality," Labour Arbitration Yearbook 1992, ed. William Kaplan et al. (Toronto: Butterworths -- Lancaster House, 1992), p. 189.

5 Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order (Pan Books: London, 1996), p. 189.

6 David H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?," in Technology and Privacy: The New Landscape, ed. Philip E. Agre and Marc Rotenberg (MIT Press: Cambridge, 1997), p. 170.

7 Nigel Waters, "Street Surveillance and Privacy," Privacy Issues Forum (New Zealand, 1996), p. 3.

8 Carl Rochelle, "Public cameras draw ire of privacy experts," CNN [webpage] March 29, 1996. Website address: http://www.cnn.com/US/9603/public_places/index.html [accessed January 21, 1998].

9 Privacy International, *CCTV FAQ*. [web page] ND. Website address: http://www.privacy.org/pi/activities/cctv/cctv_faq.html [accessed January 21, 1998].

10 Industry Canada, "Camera Surveillance in Canada", Small Town News Network [webpage] ND; Website address: http://www.arcnewmedia.com/stnn/cctv.html [accessed January 21, 1998].

11 American Journal television program (October 1997).

12 "A Well-learned Lesson: CCTV in Florida Schools." [web page] ND. Website address: http://208.208.73.45/school/dade.htm [accessed January 21, 1998].

13 Nigel Waters, Street Surveillance and Privacy, p. 9.

14 Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order. (Pan Books: London,. 1996), . p. 177.

15 C. William R. Webster, C. William R., "Closed Circuit Television and Information Age Policy Processes"; Glasgow Caledonian University, Centre for the Study of Telematics and Governance, Dept. Of Management [article draft presented to the Electronic Democracy: Discourse and Decision Making in the Information Age conference] November 10, 1997,. p. 2.

16 Michel Foucault, a 20th Century French philosopher of this century, sough, sought to extend to society as a whole, a concept of surveillance first described by Jeremy Bentham in his discussion of the Panopticon prison. The Panopticon was designed for asymmetrical (one- way) surveillance of the inmates. The inmates could always be watched but never knew when they *might* be. It was both the surveillance itself and the principle of uncertainty that were used as a means for subordination. Today, we are very familiar with this relationship of panopticism in the form of - one which CCTV systems thmselves epitomize.

17 Presentation by the Privacy Commissioner of Canada, n.d.

18 Andrew Neil, BBC-TV, May 29, 1996 excerpt in CCTV FAQ, Privacy International, ND. Website address: http://www.privacy.org/pi/issues/cctv/cctv_faq.html [accessed January 29, 1998].

19 See note 18 above.

20 Carl Rochelle, "Public cameras draw ire of privacy experts"; CNN [webpage] March 29, 1996. Website address: : http://www.cnn.com/US/9603/public_places/index.html [accessed January 21, 1998July 15, 1997].

21 KDIS Online. "CCTV - Big Brother in Bradford"[webpage] March, 1997. Website address: ; http://merlin.legend.org.uk/~brs/cctv/kdis12.html [accessed January 21, 1998].

22 KDIS Online. "CCTV - Big Brother in Bradford"[webpage] March, 1997. Website address: ; http://merlin.legend.org.uk/~brs/cctv/kdis12.html [accessed January 21, 1998].

23 Privacy International, CCTV Frequently Asked Questions, ND. Website address: Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order. Pan Books: London. 1996. p. 180http://www.privacy.org/pi/activities/cctv/cctv_faq.html [accessed January 29, 1998].

24 See Cf. Speiser v. Randall, 357 U.S. 513, 526 (U.S.S.C., 1958). So long as the statute remains available to the State, the threat of prosecutions of protected expression is a real and substantial

one. Even the prospect of ultimate failure of such prosecutions by no means dispels their chilling effect on protected expression. See also [webpage] 1965 Dombrowski v. Pfister, 380 U.S. 479 (U.S.S.C., 1965)http://caselaw.findlaw.com/scripts/getcase.pl?navby=case&court=US&vl=380&page=479 [accessed December 15, 1997].

25 Nigel Waters, "Street Surveillance and Privacy," Privacy Issues Forum (New Zealand, , 1996), p. 1.

26 See note 25 above, p. 7.Nigel Waters, "Street Surveillance and Privacy," Privacy Issues Forum (New Zealand, 1996), p. 7

27 Carl Rochelle, "Public cameras draw ire of privacy experts"; CNN [webpage] March 29, 1996. Website address: http://www.cnn.com/US/9603/public_places/index.html [accessed January 21, 1998July 15, 1997].

28 Graham, S. Brooks, J. and Heery, D. 1996.S. Graham, J. Brooks, D. Heery, " Towns on television: Closed circuit television surveillance in British towns and cities," in . Local Government Studies, Vol. 22, No. 3 (1996), pp. 1-27; C. William R. Webster, in "Changing Relationships Between Citizens and the State: The Case of Closed Circuit Television Surveillance Cameras,", C. William R. Webster p. 12.

29 Investigation Report P95-004 ("A Complaint by KF Media Inc. against the Vancouver Police Department concerning the Television Series `To Serve And Protect'"), March 22, 1995, p. 8. Website address: http://www.oipc.bc.ca/ investigations/reports/VPD.html

30 Interview with Leslie Sharp, Chief Constable for Strathclyde, Scotland, *20/20*, ABC News, September 7, 1995. Website address: http://www.privacy.org/pi/issues.cctv/cctv_faq.html [accessed February 12, 1998].

31 William Kole, "Cameras Ggive Dutch that Wwired Ffeeling," Victoria Times-Colonist, August 10, 1997,. p. A5.

32 Society for Human Resources Management, 1991 SHRM, Privacy in the Workplace survey report, Alexandria, Virginia, 1992 in Simon Davies, p. 192.

33 Louis Harris and Kamala Allsop, Equifax Canada Report on Consumers and Privacy in the Information Age (Canada: Louis Harris, 1994), p. v.

34 Honess T., and Charman E. (1992), "Closed Circuit Television in public places," Crime Prevention Unit paper no. 35, London HMSO, excerpt from Privacy International, *CCTV FAQ*, (see note 10, above).

35 Vancouver Public Library. "Central Branch FAQs" [webpage] ND. Website address: ; http://www.vpl.vancouver.bc.ca/branches/LibrarySquare/misc/faqcen.html [accessed January 21, 1998uly 15, 1997].

36 Vancouver Public Library, written submission to the Information and Privacy Commissioner of British Columbia, March 24, 1998.

37 ICBC Annual Report, 1996. Website address: http://www.icbc.com [accessed January 30, 1998].

38 Insurance Corporation of British Columbia, written submission to the Information and Privacy Commissioner of British Columbia, February 27, 1998.

39 Canadian Standards Association, Model Code for the Protection of Personal Information (Toronto: CSA, 1996); MMaking the CSA Privacy Code Work for You, (Toronto: CSA, 1996), p. 11.

40 See note 38 above.

41 CSA Model Code for the Protection of Personal Information (Q830-96), article 4.5 (Principle 5).p. 5

42 See note 40 above. CSA p. 5.