Video surveillance in public places

June 1999

Introduction

The Vancouver Police Department is proposing to jump on a bandwagon along with several cities in the UK, United States and eastern Canada, to use video surveillance, or closed circuit television (CCTV) in high crime areas. CCTV involves the placement of video cameras to monitor activity on the sidewalks, alleyways and other public places in a given area. Cameras pan the area and can be focused or zoomed in from a remote site. The cameras can be driven by motion sensors to automatically focus on citizens' movement, or be under the control of the observers who view the activities from a remote site, with those being observed completely unaware that they are being tracked, perhaps for several minutes at a time, with cameras capable of zooming in on them with a resolution capable of identifying the tattoos on their arms or the titles of the books they are carrying in their hands. The Department's original proposal called for a system of 16 cameras in the Downtown Eastside, Strathcona, Gastown and Chinatown neighbourhoods, and following preliminary public meetings on the subject, the number has already grown to 25. This is a 50% increase before the scheme has finished the consultation stage. The startup costs of the scheme are about $400,000 for the original 16 camera system.

Proponents of this technology, including the police, in their draft document, CCTV: A Community Policing Option for the Downtown Eastside (hereafter Vancouver Police (1999)), emphasize the advantages to be had from CCTV. The report quotes from a City of Vancouver document, *The Downtown Eastside Community Revitalization Program:*

The community, private sector, and governments need to commit to a long-term program of community development, and specific, targeted actions to solve problems in the area. It has been said that the community lacks a common vision. Yet, everyone wants to be able to walk the streets in relative safety, everyone wants to see a lively street scape with active businesses and services, and everyone wants the opportunity to make the best of their lives. These areas of consensus provide a basis for community development work, which will lead to successes, the feeling of accomplishment in a foundation on which to develop strategies to tackle more difficult issues. (p. 14)

The report holds that CCTV is just the thing to bring about these goals:

The advantages of CCTV, properly managed, speak for themselves: Crime prevention, the deterrent effect of knowing that there is observation, the alerting of police at an early stage to stop dangerous situations from escalating, the operational assistance to police in evaluating a situation, the safer convictions that can be obtained, the enormous savings in court time, and above all, renewed public confidence, which has led to many town centres being revitalized.

But how likely is it that these goals, laudatory as they are, will be achieved by the use of CCTV? It is the BCCLA's position that CCTV will not, even with the stringent safeguards promised in the report, achieve these goals to the degree that would justify the infringement on personal privacy that they would necessarily bring about. The cost to personal privacy must not be underestimated, and it is the BCCLA's position that the introduction of CCTV would be a cure that is far worse than the disease it is attempting to control.

We also question the rationale for this proposal coming at a time when crime rates are falling in Vancouver. The "disease" is already on the decline, in part thanks to other worthwhile measures

taken by the police, such as community policing, and in part due to changing demographics. There are simply fewer people in the group most likely to commit the types of crimes CCTV might observe; that is, males between the ages of 16 and 30. This raises the question whether a motivation for CCTV is the control of such legal but annoying activities such as panhandling.

B. Privacy in a Public Place

It might be argued that since a sidewalk, plaza or street is a public place, people do not have a reasonable expectation of privacy in these places. This objection invites us to think of the public promenades of the previous century, where people went to observe and be observed, or their late-twentieth-century equivalents, the shopping malls and sidewalks in front of convenience stores that serve the same function for teenagers.

In these places some people come to them precisely to be observed, and so it is absurd to think that someone's privacy is wrongfully invaded if they are observed there. Of course it is true that these are not private places in the way that one's living room is a private place; but it does not follow from this that no questions about invasions of privacy arise in such places. Stalking is one such example. It is not easy to draw lines between that which is permissible and that which is not in all cases. For example, consider the case of a person who decides to take different path than his usual one in order to observe someone as he walks behind the person. In the extreme case where this action was repeated, this could be considered stalking, but in other cases, for example when the route is no further than the alternative and still takes the follower to his previously chosen destination, and a person is not intrusive in his observation, this would not be the type of invasion of privacy that state should concern itself with. But the fact that there are gray areas does not prevent us from settling the cases on the extremes. As well, this argument neglects the fact that some people choose to exercise their privacy by being an anonymous individual in a crowd, subject to the casual glance of a stranger but not the scrutiny of some one trying to determine what they are up to. Casual glances are one thing, prolonged observation by someone in authority is quite another.

The same point holds for video surveillance or peering at someone through binoculars from a place where one cannot be observed doing so. What makes these activities prima facie objectionable is the built-in asymmetry of privacy involved. The watcher has her privacy preserved, in that the watched person cannot observe back, nor is he even aware that he is being observed; whereas the situation is reversed from the standpoint of the person being watched. (The point of the qualification "built-in" is that there may also be an asymmetry when Aloysius observes Sally in a public place but Sally does not notice since she is not looking in Aloysius's direction. The reason this is not objectionable is that Sally could turn around and observe Aloysius staring at her. It is just this reciprocity which is missing in the case of surreptitious viewing through binoculars or viewing someone on a video monitor the next day.)

This asymmetry of privacy is especially important when police are the watchers. Police officers have a difficult task to be vigilant enough in their observation of the streetscape to deter crime while not intrusive of individuals' privacy and the carrying out of their legitimate business. What makes finding the right level of observation easier for the individual officer is to be doing their observation publicly, where excesses can be immediately noticed by those being observed and

other people at the scene.

An officer who, with no justification, follows an attractive woman, or members of a racial or ethnic group such as Hondurans who were recently targeted by the New Westminster police, or an unaggressive panhandler, can be seen by everyone in the vicinity to be overstepping his authority. But the person monitoring a CCTV is under no constraint by those being watched. The only constraint is the worry that an audit of the videotape by a supervisor or agent of the Information and Privacy Commissioner may happen to review that five minute segment of miles of videotape before it is erased.

We should not be led down a slippery slope by arguments that suggest that, because there is nothing wrong with private individuals or the media using video cameras in a public place, we must therefore accept the proposals outlined in Vancouver Police (1999). First of all, in the former case the camera and its operator are in public view, and individuals can avoid stepping into the range of a camera trained on a building or another group of people, and can see when the cameras are trained on them or tracking them for prolonged periods, and take action to defend their privacy. Second, the cameras are on for a relatively short period of time, covering a relatively small space, as opposed to the police proposal for cameras covering at least a 59 block area 24 hours a day.

Nor should we fall for a second slippery slope starting with video cameras in places such as banks or privately-owned stores and ending with the proposal put forth in Vancouver Police (1999). In the former case, the purposes of the cameras are narrow in scope to prevent vandalism or theft from private property, as opposed to social control by the authorities. We shall return to this point in a later section.

A third slippery slope starts from the use of video cameras by public bodies to monitor traffic patterns or autos running red lights. In these cases it is the autos that are being monitored, and in the second case pictures are recorded only when a traffic offence is committed. This is a very different story from the situation where the activities of ordinary citizens are recorded as they go about their legitimate business on a public sidewalk.

A fourth slippery slope begins with the video cameras at SkyTrain stations and claims that there is no difference between this and cameras on street corners. But there is a real difference here, in that the cameras in the stations serve other purposes than prevention of violence or robbery. Given that there is no driver on the trains, there is a safety issue that provides justification for these cameras. A person who gets his shirttail caught in the doors, or who slips between two cars would be spotted by a conductor on the Toronto subway; and we would hope by a camera on SkyTrain. To be sure, SkyTrain cameras provide security to passengers traveling at non-peak periods, but it is their choice whether to avail themselves of this by standing in the clearly marked areas constantly monitored by the cameras, as opposed to being occasionally monitored by the other cameras for the average of three minutes they wait for a train at non-peak times, as opposed to being monitored for perhaps hours while shopping in Gastown, with no choice of going into a camera-free zone on the public street. As well, the SkyTrain cameras do not have the capacity to track individuals who are unaware of the cameras zooming in on them.

A fifth argument often put forth by those who see no serious concern about CCTV holds that those of us who are going about our legitimate business in the CCTV area have nothing to hide, and so we should welcome the increased security with no worries about our privacy being invaded without fearing the loss of anything we are legitimately entitled to. But this argument rests upon a confusion about our motives for wanting something to be kept private. It is simply not the case that the only reason for wanting privacy is to be able to do something that we shouldn't be doing. Thought about our eliminative functions should disabuse ourselves of this confusion. Of course, we do not perform these functions on the street; but some of us visit shops providing electrolysis for hair removal or ones providing hair transplants, and in neither case do we wish to be recorded doing so by a camera which pans the storefront. Some of us visit adult literacy centres, drug counselling centres, herbal remedy stores, debt counselling services, a psychiatrist, urologist or a weight loss clinic--all legal pursuits, but not ones everyone feels comfortable about providing testimonials on TV for them. And to be on camera without the fee is an even greater loss.

A sixth argument for Vancouver adopting CCTV technology holds that this is a policing trend that has been adopted in other jurisdictions, such as the UK or the United States. But we must remember that the former attempted to justify its adoption of this technology by the hope that it would reduce terrorist bombings, and many localities in the U.S. faced gang warfare involving guns. There are indeed risks to public safety that justify a limitation on privacy which is a consequence of a system which actually does work to reduce these risks; but we must ask ourselves whether the risks faced in Vancouver really overbalance our right to privacy. Note that the BCCLA is not maintaining that CCTV is always an unjustifiable offence against privacy; but what raises the question is that it does not involve the notion of reciprocity involved in the expression "to observe and to be observed". In the next section we introduce some principles designed to distinguish those cases where such asymmetric observation is justifiable from those where it is not.

C. Criteria for Acceptable Video Surveillance in Public Places

In order to be acceptable, video surveillance of a public place must:

1. Fulfill an important purpose such as reduction of risk of physical harm or other illegal activities and not simply the control of nuisance such as panhandling;

2. Not simply drive a problem from one area into another area that does not have video surveillance;

3. Be less invasive of privacy than alternative means of surveillance;

4. Be advantageous to all or at least to most of the people who are giving up their privacy;

5. Provide the public with clear notification of the its presence in the areas where surveillance occurs, a publicity campaign in the media to inform people of the locales where it is located, etc.);

6. Inform the public of its rationale;

7. Inform the public about who is monitoring the cameras, what use is to be made of the tapes, how long they are to be stored, etc.;

8. Be monitored by the Information and Privacy Commissioner with respect to its deployment and the use and storage of the tapes it generates;

9. Fulfill its promise as a means of identifying suspects;

10. Not be used as part of a data matching program for purposes other than surveillance for the reduction of crime of the area in which it is installed;

11. Be more efficient in terms of cost/benefit (in terms of loss of privacy, expense, and effects on other resources on the cost side, and increased security on the benefit side) than alternatives.

These criteria are meant to apply to the use of CCTV in a public place by public bodies such as the police. Although it is not the subject of this brief, most of them apply mutatis mutandis to private organizations using CCTV in areas such as department stores and instant teller machines. The modifications required to these criteria when applied to private as opposed to public places are; to Criterion (1), to include the private interest of the company installing the cameras to prevent vandalism or theft of their property, Criteria (3), (4) and (11), where, as long as the public is properly informed that the video surveillance is in place, may choose to trade their privacy for cheaper prices or to go elsewhere, and so the requirement for benefit to the consumer is less strict. Criterion (2) does not apply to private organisations at all; private individuals and corporations have the right to defend themselves against theft or vandalism of their own property even if their security measures drive thieves and vandals to their less security-conscious neighbours. It is the job of the police and other government organizations to provide general security for the whole community, but this ought not to prevent individuals, within limits, from defending their own property. (4) and (8) raise a special issue of concern to the BCCLA. It is our position that fair information practices incorporated into federal and provincial legislation such as B.C.' *Freedom of Information and Protection of Privacy Act* ought to apply to private organizations as well as to the government. This is presently not the case, though this might change with the introduction of Bill C-54, the *Personal Information Protection and Electronic Documents Act* in the federal parliament. But this is an argument to be taken up in another place.

D. Tradeoffs of Privacy for Safety

Privacy is one such good amongst many; and at some point some set of other goods will be of more value to an individual than privacy. Furthermore, there is room for rational people to disagree, within limits, on the values of these goods. The problem can become difficult, then, when we must decide on a social policy or program such as CCTV which imposes different costs and benefits on different individuals, given their differing situations and priorities. However, where the losses clearly outweigh the gains, skepticism about the ability to rationally measure these losses has academic interest but little practical worry. In this section, we maintain that the considerations discussed below make it clear that the introduction of CCTV result in relatively

little benefit, and at such a large cost that it cannot be justified. The major cost is to our privacy, and the major gains that are promised are in terms of increased safety. *(1) Serious v. lesser harms*

If people are to give up their privacy for CCTV, they must be guaranteed that they receive a tangible benefit in exchange. Not only this, but the benefit must be something they are entitled to in a public place. It is the position of the BCCLA that people are not entitled to be free from being politely approached by panhandlers or religious cult members offering tracts, or seeing people who look like they might go into an alleyway to shoot drugs, unless they are physically accosted by them, notwithstanding that local merchants are convinced these people are bad for the tourist trade, and therefore citizens should be prevented from these activities by state action.

But Vancouver Police (1999, pp. 38 and 46) shows clearly that the regulation of nuisance is high on the agenda of proponents of CCTV. From the discussion of the tables on these pages, the police maintain that CCTV would be useful in drawing to the attention of the authorities 7,464 of the 21,192 calls for service in the area covered by CCTV. But of the 7,464, 2,797 (p. 38) or 37% fall into this 'nuisance' category (person annoying, suspicious circumstances, suspicious person, mental case and parking complaint). To be fair, 430 calls in this category were for "person down", some of which no doubt were for someone who was ill, but many of which were for drunks who will be simply "moved along", not given medical attention. As Fredericks says, "these calls were for matters which could have been diverted to private security for initial response".

This quote raises another worry: Given that, as mentioned above, the FOIPP Act does not cover private organizations, the police must ensure that any information traded with private organizations will be treated in the same way the Act requires them to treat it. But at present, the Information and Privacy Commissioner has no powers to deal directly with those private organizations.

(2) Crime reduction v. displacement

Proponents of CCTV, including Fredericks (1999), claim that it has shown to be an effective crime deterrent. However, the studies cited to establish this claim do not provide much evidence for it. The studies cited suffer from two major problems which are not adequately controlled for the Hawthorne Effect and Displacement. The first refers to a problem which plagues any study of human behaviour. The mere fact that the behaviour is studied influences the behaviour which is studied, in the short term. In the case of CCTV, the fact that there will be researchers monitoring the cameras and the neighbourhood, and technicians adjusting the cameras is itself likely to diminish crime in the short run as the system is installed and fine-tuned, given the presence of people hanging around with clipboards, cases of wires and pliers and the like. Even when researchers are not present, the novelty of the system will for a time deter crime. But over time the novelty wears off, criminals learn where the blind spots of the cameras are, and crime will revert to its previous levels. Thus a short survey period will show a sharp decrease in crime, but a longer one will show the increase back to previous levels. Many of the studies cited by proponents of CCTV are of too short a duration to give an accurate assessment of CCTV's actual deterrent effect.

The second problem, displacement, refers to the possibility that, while crime will decrease in the areas where the cameras are located, it will increase in surrounding neighbourhoods due to the fact that criminals simply move to a new neighbourhood which is not monitored. These two problems exacerbate a third problem which is the general lack of proper controls. For example, many of the studies do not control for a general drop in crime in the city in question. That is, some studies indicate a drop in crime in the areas where cameras are located, but do not take into consideration diminishing crime rates in the entire city. Nor do they account for the effects of other programs instituted at the same time in the areas where the cameras are located. Cameras are, naturally, located in high crime areas where police are perennially concerned about crime. Thus, they embark upon a number of other crime reduction strategies, such as more street patrols, neighbourhood watch, etc., at the same time they install the cameras. Unsurprisingly, crime rates fall; but how much of this is due to the cameras is beyond the power of the surveys to determine. Sometimes the explanation for these problems in the studies is that they are done by those with a vested interest in showing the effectiveness of the cameras the police, those companies selling the cameras, or the business groups who desperately want to believe that this new technology is the panacea for their perennial crime problem. In other cases, it is just plain difficult to control for these other factors.

The Hawthorn Effect not only raises methodological issues pertaining to the evidence that CCTV has a long-term effect on crime, it also suggests that the effects CCTV will have on crime reduction are contingent upon its continuing use; and thus its long-term invasion of privacy.

The problems with displacement raise serious worries about the long-term effect on privacy that will result from the use of CCTV. If CCTV merely results in criminals moving to another area, the only way to have a meaningful effect on overall crime rates is for it to spread throughout the whole city. This has in fact been the case in the UK, where there were as of 1995 more than 200,000 cameras, and estimates of up to 400,000 presently in use. And, as we noted in the Introduction, the Vancouver proposal has increased by 50% before the first camera has been installed!

These results come as no surprise when society tries to deal with the negative spin-offs of the drug trade, not by means that address the drug problem directly, but by a quick technological fix. Ironically, CCTV has features resembling the very drug problem it is usually invoked to solvelike addiction, CCTV requires heavier and heavier doses for it to continue to have any effect. Thus, those who fear that the introduction of CCTV is the thin edge of the wedge leading to greater and greater invasions of privacy are on solid ground. This in turn suggests that CCTV cannot mean a relatively cheap, limited answer to the problems of crime. For this reason the proponents of CCTV must conclusively refute the argument from displacement. The study attempts to answer the charge that CCTV merely displaces crime with a very weak argument:

> In fact, here in Vancouver, police have found that at least half of the criminals arrested in the Downtown Eastside, do not live in the area. They go there to commit crime. A CCTV system could prove an effective deterrent to visiting criminals. (p. 29)

But this misses the point. The criminals could simply visit somewhere else if the Downtown Eastside were to become too hot for them. As British police officer Wesley Sharp put it, "Certainly the crime goes somewhere. I don't believe that just because you've got cameras in a city centre that everyone says 'Oh well, we're going to give up crime and get a job.'" (CCTV

The third argument against CCTV, the failure to account for confounding variables, suggests another objection to CCTV. If much of the crime prevention noticed in the studies is in fact due to other measures taken along with CCTV, then implementing these other measures without CCTV would be about as effective, without the large costs of CCTV in terms of both money and invasion of privacy. As Anatole France put it, "The casting of spells and anthrax has led to the death of many cattle".

(3) Lesser invasion of privacy than alternatives

As we argued in the Introduction, CCTV, given the asymmetry of privacy necessarily involved in it, clearly does not satisfy this condition. Police officers on the street do tend to intrude to a degree on individuals' carrying out of legitimate activities, but they also provide many immediate benefits, such as directing tourists to the Steam Clock and warning a parent that a child is starting to wander. And, as we have previously mentioned, when they exceed their legitimate authority they can be seen to be doing so; they are not watching us from a secluded basement.

(4) Advantages to those giving up their privacy

It is unrealistic to expect that everyone should benefit equally from the introduction of a new social policy or program, or even that their benefits over losses be equal. But almost all moral theories require that those at the bottom not be the ones suffering a loss in order to provide a gain for those who are better off. (Rawls' theory of justice (Rawls, 1974) states this as a formal requirement of the theory, and Utilitarianism requires it about as universally as anything is required in utilitarianism when the effects of Diminishing Marginal Utility are taken into account.) In any event, common morality requires that those who suffer a disproportional loss for others' gain can see that their loss is required for the wider social good.

CCTV in Vancouver's Downtown Eastside fails to meet even a generous interpretation of these requirements. There are three types of people affected by CCTV in a limited area:

a. those who live in the area but spend a good proportion of the day (working, &c.) in an area not covered by CCTV;
b. those who live outside the area covered by CCTV but spend a good portion of their day in the area; and
c. those who both live and spend most of their time in the area.

Given the Displacement Argument outlined above, those in groups (a) and (b) gain little if the crime done to them occurs, not in the CCTV area but in the other area(s) where they spend their time. Even if they gain something from the reduction in crime in the CCTV area , this must be balanced against the invasion of privacy they must put up with while in the CCTV area. For most people, we submit, with this last cost filtered in, they will probably lose. The gainers will be the people who frequent the CCTV area only rarely and live in a neighbourhood to which the crime has not been displaced.

It might be thought that those in group (c) gain the most a satisfying result, since they tend to be the worst off in the community but this would be a mistake. First of all, they lose the most from the invasion of their privacy since they spend the most amount of time in the CCTV area. And second, they lose more of their privacy than many other people in the area because of what makes them the worst off in society. If they live in a dreary SRO hotel, they spend a far greater portion of their day outside under the gaze of the camera than those working in a shop. And living in the area is highly correlated with being a member of a group most likely to be targeted by a panning camera because they are the most suspicious in the eyes of those panning the camera. Native, indigent-looking or other people are far more likely to be targeted than someone in a suit. We shall say more of this in our discussion of criterion (9) below.

Now, there may be some residents in the Downtown Eastside who judge themselves gainers from the increased security offered by CCTV, even at the cost to their privacy. But they may not be in the majority. A recent *Vancouver Sun* article pointed out that a large number of the assaults in this area occur, not on the streets, but in rooming houses or other areas not covered by the cameras. In fact, the article suggested that a larger percentage are occurring indoors because of the increased presence of police on the streets. Of course minimizing these assaults is of the greatest public concern; but it is not clear that CCTV is the answer to this problem.

E. Criteria Covered in the Freedom of Information and Protection of Privacy Act

Criteria (5)--(8) are the ones covered in B.C.'s *Freedom of Information and Protection of Privacy Act*, and come under jurisdiction of the Information and Privacy Commissioner. This point is clearly recognized by both the Information and Privacy Commissioner (Flaherty 1998) and Vancouver Police (1999). The Act requires criteria (5) (8), and in addition, since the videotapes constitute a record, must be disposed of properly (in this case, properly degaussed (completely erased) before disposal). The Act also requires that individuals have the opportunity to view a record that is used in a decision concerning them, and therefore it requires that tapes be retained for at least a year if they are to be used against a person.

Nevertheless, there are two worries. First, there is the practical problem with the Information and Privacy Commissioner being able to effectively monitor CCTV on a daily basis. And the second has to do with criteria (5) and (6). Where a CCTV device is present at an instant teller machine or the entrance to a building, it is relatively easy to post signs warning people of its presence. The space is relatively confined, and the notice can be easily spotted by people using the service. Since they pass through the area relatively quickly they can remember that they are in range of the camera while they are there. But when CCTV covers an entire district, as is proposed here, people can easily enter into the area without seeing the notice. And even if they notice a sign upon entering the area, it is easy for them to forget its presence. Many shoppers, for example, will spend several hours in the area, going in and out of shops, thinking about their purchases or other matters, and can easily forget that they are under surveillance. The amount of signage required to counter this would be enormous, and would itself leave citizens with the feeling that they have entered the world of *The Prisoner*.

F Identifying suspects and data matching

(9) Identifying suspects

One of the hottest areas in artificial intelligence research is that of devising artificial intelligence programs for facial recognition. To date, the machines do far too poorly on these tasks to avoid miscarriages of justice if their 'identifications' were to be relied upon in criminal proceedings. A large part of the problem is that computers rely on the same two-dimensional images that are produced by a videotape. Where machines must make their identifications from images of people where the face is at an angle, or has a different expression, their success rates are intolerably inaccurate. However, a recent study reported in the New Scientist (1999) suggests that the reason machines do so poorly is that humans are not very much better:
Vicki Bruce of the University of Sterling and Mike Burton of the University of Glasgow tested the ability of 230 Open University students to match pictures of faces grabbed from video with still photographs of 10 similar faces. The faces, which were all young, the clean-shaven short-haired Caucasian males, were pulled from a home office database of 200 trainee police officers.

To their surprise, Bruce and Burton found that even in ideal conditions using high-quality pictures, full-frontal faces and neutral expressions only 70 percent of identifications were correct. When the face grabbed from the video was smiling, the proportion of accurate matches dropped to 64 percent. When it was shown at an angle of 30 degrees, the figure was only 61 percent. Thus the touted advantage of video monitoring for identification of suspects is called into question by the actual data. But the problem gets worse. Reporting on another study of Bruce and Burton the article states:
However, other experiments showed that when faces caught on poor quality video were familiar to the student volunteers over 90 percent of their identifications were correct.
"Over 90 percent" is one and a half times better than 61 percent; but we shouldn't let this higher figure lead us to think that video identification under CCTV is not likely to produce a travesty of justice in a large number of cases. Extrapolating these data to the real world of identification of suspects from video, and adding to them the extensive data provided by Loftus (1979) that people's expectations influence their perceptions and memories, we are faced with a dilemma. Where police or witnesses view video images of people unknown to them, their perceptions are not much better than flipping a coin. But where the image on the video is known to the identifier in the sense of being someone suspected of having just robbing one's store, or of a police officer trying to identify that troublemaker they've been watching for years, the identification from a video image of a face taken from an odd angle this identification may be less accurate than flipping a coin. Our expectations in the latter case can cause even trained perceivers to read into fuzzy images what we think, on the basis of other evidence, we think we should see. And what makes matters even worse is that, as the *New Scientist* (1999) puts it, quoting from a psychologist expert in video identification, "it bestows a kind of spurious scientific glitz on identification". Because we are not relying on our own judgment, which we know to be fallible, but on a high-tech gizmo which we think to be infallible, we express our judgments with a far higher degree of confidence than we are entitled to. In other words, CCTV is the visual analogue of the polygraph as a policing tool.

(10) Data matching

Flaherty (1998 and 1999) raises the worry of the data from video images from CCTV being combined with other records—credit card receipts, PharmaNet records or police incident files, to name just three—to bring about a "surveillance society" in which citizens' legitimate movements are tracked and dealt with. Obviously some citizens political dissidents or those with an alternative lifestyle are at a greater risk than others. The BCCLA shares these concerns. In addition, we have the concerns of the previous subsection about the accuracy of identification of individuals from CCTV.

It is hard to say whether the greatest harm from such data matching would come about in the short run where people will be falsely accused of being in a certain place at a certain time about as often as they are correctly tracked, or in the long run when the technology improves and they are accurately tracked.

G. Costs v. benefits

Even if we confine ourselves to the monetary costs of CCTV, the experience of the UK (which in 1995 was estimated to have spent up to 300,000,000 per year on CCTV) noted above should remind us that as the initial promise of CCTV is not met, the usual answer is to simply spend more on it to attempt to derive the expected benefits. And we have noted above several reasons for doubting that CCTV is capable of delivering the benefits its proponents are looking for. But when we add to this the costs of invasion of privacy of innocent people going about their business in a public place, the introduction of CCTV in Vancouver's Downtown Eastside or anywhere else in the city for that matter is entirely unjustified.