PUBLIC VIDEO SURVEILLANCE BY THE STATE: POLICY, PRIVACY LEGISLATION, AND THE *CHARTER*

DEREK LAI*

This article explores the growing phenomenon of public video surveillance and how the law should protect an individual's right to privacy while providing for effective law enforcement. The author considers the positive and negative effects of surveillance and recent technological advancements that currently challenge courts, legislatures, and police forces. Canadian case studies from Kelowna and Edmonton are utilized to examine the role of federal and provincial privacy legislation, while the Supreme Court of Canada's evolving interpretation of s. 8 of the Charter *is canvassed through an examination of jurisprudence involving public surveillance technology. Ultimately, the author concludes that public video surveillance is necessary but the law must control its use. Video surveillance via automated collection would resolve the "effectiveness versus privacy" policy debate by minimizing the potential for abuse.*

Cet article explore le phénomène grandissant de la vidéosurveillance publique et de quelle manière la loi devrait protéger les droits à la vie privée tout en appliquant efficacement la loi. L'auteur examine les effets positifs et négatifs de la surveillance, ainsi que les récents progrès technologiques actuellement devant les tribunaux, le parlement et les forces de police. Les études de cas canadiens de Kelowna et d'Edmonton sont utilisées pour examiner le rôle des lois fédérale et provinciales sur la protection de la vie privée, alors que l'interprétation évolutive de la Cour suprême du Canada de l'article 8 de la Charte est discutée par l'examen de la jurisprudence sur la technologie de la surveillance publique. En définitive, l'auteur conclut que la vidéosurveillance publique est nécessaire mais que la loi doit en contrôler l'utilisation. La vidéosurveillance par la collecte automatique pourrait régler le débat sur « efficacité contre protection de la vie privée » en réduisant le potentiel d'abus.

TABLE OF CONTENTS

* Student-at-Law, Alberta Court of Appeal and Field Law in Edmonton, Alberta, then returning to the Edmonton Police Service as an in-house legal advisor. This article received one of the top awards for the 2007 Morrow Essay Contest.

I. INTRODUCTION

In 2002, the Privacy Commissioner of Canada declared video surveillance of public places to be the "most urgently important privacy issue facing Canadian society today."[1] The proliferation of cameras operated by the police posed a serious danger to the privacy essential to maintaining a free and democratic society,[2] and former Privacy Commissioner George Radwanski called for a cessation of this type of surveillance. Since then, more Canadian police agencies have deployed public video surveillance (PVS) as a possible solution to crime and disorder, and this will undoubtedly continue with the technology's expanding capabilities. Urgent answers are thus needed as to whether this surveillance is legal under federal and provincial privacy legislation, and whether it will likely engage the *Canadian Charter of Rights and Freedoms*.[3]

The goal of this article is to provide a comprehensive overview of the issues surrounding the police use of video surveillance in public areas such as streets, city centres, and parks. Part II discusses the policy debate surrounding the effectiveness and privacy impact of PVS. Part III provides a comparison between two Canadian closed circuit television (CCTV) experiences, one falling under federal privacy legislation, and the other subject to Alberta's privacy legislation. Part IV is an analysis of how PVS constitutes a search under s. 8 of the *Charter*, and whether or not it may be utilized "reasonably" in order to comply with s. 8.[4]

II. THE POLICY DEBATE: EFFECTIVENESS VS. PRIVACY

The policy debate regarding police video surveillance of public areas is usually framed as a balance between effectiveness and privacy: does its positive effect on crime outweigh its negative impact on privacy? For former Privacy Commissioner Radwanski, the answer was clear: "there is absolutely no evidence that video surveillance cameras on public streets are effective in reducing or deterring crime,"[5] while at the same time, it posed a "dramatic new intrusion on privacy."[6] But general video surveillance is a relatively new phenomenon whose impact on crime and privacy is complex and, to a large degree, still undetermined. Moreover, technological progress means that there must be constant re-evaluation of this balancing equation. And while state cameras intuitively seem to pose a serious danger to privacy interests, in order to determine why and how privacy is threatened, it is necessary to unravel its features.

---

1. George Radwanski, Privacy Commissioner of Canada, "Watching You: Privacy Rights and Video Surveillance" (Address to McMaster University, Communications Studies Programme, 13 February 2002), online: Office of the Privacy Commissioner of Canada (OPC) <http://www.privcom.gc.ca/speech/02_05_a_020213_e.asp>.
2. *Ibid.*
3. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [*Charter*].
4. *Ibid.*
5. OPC, News Release, "The Privacy Commissioner of Canada, George Radwanski today sent the following letter to the Honourable Lawrence MacAulay, Solicitor General of Canada, regarding video surveillance by the RCMP" (15 March 2002), online: OPC <http://www.privcom.gc.ca/media/nr-c/02_05_b_020315_e.asp>.
6. *Ibid.*

A. EFFECTIVENESS

1. THE GOALS OF PUBLIC VIDEO SURVEILLANCE

We can assess the effectiveness of PVS in terms of its goals: deterrence, detection, evidence gathering, police deployment, and decreasing fear of crime.

a. Deterrence

Welsh and Farrington's 2002 meta-analysis for the British Home Office is probably the most extensive and reliable evaluation of CCTV.[7] The authors considered 46 CCTV studies from the United Kingdom and North America but excluded 24 because they were not methodologically sound.[8] The authors drew the following conclusions from the remaining 22 studies.

First, CCTV resulted in only a general 4 percent reduction of crime. Eleven of the studies found a significant reduction in crime, whereas five actually found an increase in crime, five found no effect on crime, and one found an uncertain effect on crime. Moreover, the positive evaluations all came from British CCTV systems, whereas the North American studies found either a neutral or negative impact on crime.[9]

Second, the effectiveness of PVS varied according to three types of environments. For city centres and public housing, CCTV had a negligible 2 percent reduction in crime. On public transportation systems, there was a non-significant 6 percent reduction in crime. CCTV proved most effective in parkades, which experienced a 41 percent drop in crime compared to control areas.[10] However, the authors pointed out that the parkade systems only had a significant impact on vehicle crimes, which was the only crime type measured. And, all the car park systems were part of a larger crime prevention campaign that included additional interventions such as improved lighting. The video surveillance of city centres and public housing were almost all stand-alone measures.[11]

Third, the impact of CCTV varied across crime categories. It had little or no effect on violent crime, but a significant impact on property crimes, especially crimes relating to vehicles.[12] A subsequent 2005 Home Office study by Gill and Spriggs further concluded that CCTV was less likely to reduce impulsive and/or alcohol-related crimes as compared to premeditated crimes such as car theft.[13]

---

7 Brandon C. Welsh & David P. Farrington, *Home Office Research Study 252 — Crime prevention effects of closed circuit television: a systematic review* (Home Office Research, Development & Statistics Directorate, August 2002), online: Home Office Research, Development & Statistics Directorate (Home Office) <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>.

8 *Ibid.* at i.

9 *Ibid.* at vi.

10 *Ibid.* at vi-vii.

11 *Ibid.* at vii.

12 *Ibid.* at vi-vii.

13 Martin Gill & Angela Spriggs, *Home Office Research Study 292 — Assessing the impact of CCTV* (Home Office Research, Development & Statistics Directorate, February 2005), online: Home Office <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf> at vii.

Critics often argue that general video surveillance merely displaces crime into areas outside the camera's range. Whether this is actually the case remains uncertain. In the 2005 Home Office study, Gill and Spriggs considered 13 CCTV systems.[14] Most did not manifest any displacement effect. However, one program appeared to generally displace crime into the surrounding area, while one system showed only displacement of break and enters, and another showed displacement of vehicle crime.[15] It should be noted too that displacement can sometimes be a positive phenomenon which prevents crime from becoming entrenched in a particular neighborhood. And some studies argue that the benefits of PVS can actually be "diffused" to neighboring areas.[16]

b. Detection

If PVS has a deterrent effect, then it should prevent crime from happening in the first place and crime rates should decrease. But if the surveillance increases the chances of detecting offences as they occur, it should also drive up crime rates, at least at first. Therein lies another difficulty with relying on crime rates as a measure of effectiveness. Eventually, one would expect that increased detection would also have a deterrent effect, so that any initial rise would be followed by a drop in crime rate.

But more work must be done to isolate the impact of PVS on detection. A 2003 literature review of CCTV evaluations conducted by the Royal Canadian Mounted Police (RCMP) found that there was a deficit of scientific research on the direct effects of CCTV on detection, arrest and conviction of offenders.[17] While it is logical to infer that video footage will assist in the apprehension of criminals, statistics would give us a better idea of the extent of this effect, and whether the benefit is worth the effort.

c. Evidence Gathering

Police have long used video footage from privately-operated surveillance cameras to investigate crimes and prosecute offenders. One would assume that this would translate to state-operated video surveillance in public places, but again, there is a lack of statistical analysis in this area. One would further expect that gathering evidence would positively affect deterrence and detection, but the relationship remains unclear. The value of video may extend even beyond the immediate apprehension of the offender and could ease the burden on the criminal justice system if those accused, facing powerful video evidence, are more likely to plead guilty rather than go to trial.

---

14 *Ibid.* at v.

15 *Ibid.* at vii.

16 Coretta Phillips, "A Review of CCTV Evaluations: Crime Reduction Effects and Attitudes Towards Its Use" in Kate Painter & Nick Tilley, vol. eds., Ronald V. Clarke, series ed., *Crime Preventions Studies — Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*, vol. 10 (Monsey, N.Y.: Criminal Justice Press, 1999) 123 at 128.

17 Wade Deisman, *CCTV: Literature Review and Bibliography* (Ottawa: Research & Development Branch; Community, Contract and Aboriginal Policing Services Directorate; Royal Canadian Mounted Police, 2003), online: RCMP <http://www.rcmp-grc.gc.ca/ccaps/research_eval_e.htm> at 16.

d. Deployment of Police Resources

Police often argue that street video surveillance helps them respond more efficiently, effectively, and quickly to incidents in progress, and that this assistance in turn should help detect and deter crime. Again, only anecdotal evidence is offered to support this claim. For example, a study completed by the Edmonton (Alberta) Police Service of their own PVS program described a gun complaint where the monitor kept sight of the suspect on the video screen, directed officers to his location, and notified them of where on his person he had hidden the gun.[18] The evaluation of the Sudbury (Ontario) Regional Police Service's Lion's Eye in the Sky video monitoring project reported instances where monitors kept an eye on police officers during traffic stops, and, in some cases, dispatched back-up even before the police officer had requested it.[19]

e. Decreasing the Fear of Crime

While PVS possibly only makes citizens feel safer without actually reducing crime, some point out that the fear of crime has a significant effect on a person's quality of life, and thus measures which alleviate that fear are worthwhile.[20] Indeed, despite the fact that crime rates in Canada have been falling since 1991, a 1999 survey found that 29 percent of Canadians believed that crimes rates had risen, while 54 percent believed that crime rates had stayed at the same level.[21] Moreover, reducing the fear of crime may often reduce crime itself. People may lose their reluctance to enter problem areas because they are less fearful of crime, which might promote the "natural surveillance" which deters crime from happening in the first place.[22]

Whether PVS actually reduces the fear of crime, especially over the long term, is questionable. The 2005 Home Office analysis found that citizens generally worried less about being a victim of crime in a CCTV-covered area, but this was statistically significant in only 3 of the 13 areas. Worries about being generally affected by crime showed a significant reduction in just two areas. Following the installation of CCTV, general feelings of safety did increase in all but one of the areas, but none of these results were statistically significant.[23] In terms of general support for CCTV, the meta-analysis found that the proportion of people who were happy or very happy with the surveillance declined in nine

---

18 Cst. Jay Reinhelt & Cst. Alex Thomas, *Whyte Avenue CCTV Review — Old Strathcona Closed Circuit Television Camera System* (Edmonton Police Service, 2003) [unpublished] at 2.

19 KPMG, *Evaluation of the Lion's Eye in the Sky Video Monitoring Project* (Sudbury, Ont.: KPMG, 2000), online: Greater Sudbury Police Service <http://www.police.sudbury.on.ca/publications/reports/KPMG.pdf> at 2.

20 Robert W. Hubbard, Susan Magotiaux & Matthew Sullivan, "The State Use of Closed Circuit TV: Is There a Reasonable Expectation of Privacy in Public?" (2004) 49 Crim. L.Q. 222 at 240.

21 David Loukidelis, Information & Privacy Commissioner for British Columbia, "Privacy and Law Enforcement — Getting the Balance Right" (Address presented to the 24th Annual Training Symposium, BC Crime Prevention Association, Surrey, B.C., 19 September 2002), online: Office of the Information & Privacy Commissioner for British Columbia <http://www.oipcbc.org/pdfs/public/BCCrimPrev091902.pdf> at 10.

22 *Supra* note 20.

23 Gill & Spriggs, *supra* note 13 at viii.

areas after the system was installed. This decline was statistically significant in five of those areas. Nonetheless, general levels of support exceeded 70 percent in all but one of the areas.[24]

The success of PVS in reducing fear of crime will no doubt be dependent on the political, social, and cultural context. Canada has not experienced the urban disorder and terrorism seen in the U.K. or the United States. Moreover, Canadians have strong attitudes about their civil liberties and general distrust of police appears to be rising, such that police-controlled PVS could actually make citizens more fearful rather than less.

2. CANADIAN EVALUATIONS OF PUBLIC VIDEO SURVEILLANCE

Two studies of Canadian CCTV projects, Sudbury Regional Police Service's Lion's Eye in the Sky Video Monitoring Project in Ontario and Edmonton Police Service's Old Strathcona CCTV System in Alberta, provide insight into how PVS functions in a Canadian context.

a. Sudbury Regional Police Service — The Lion's Eye in the Sky Video Monitoring Project

Sudbury's Lion's Eye in the Sky project began in 1996 with a single camera, and expanded to five cameras covering the downtown area over the next three years. The cameras always recorded, but were occasionally unmonitored. In those instances, the cameras followed pre-programmed scanning patterns.[25]

In 2000, a KPMG evaluation found a dramatic decrease in the crime rates for the downtown area. Prior to the PVS program, there had been two years during which violent crime increased. During the first three years of the program, the number of assaults and robberies decreased by 38 percent. Property crimes had been decreasing gradually in the five years before the Lion's Eye in the Sky project but after its implementation, they dropped by 44 percent from 1996 to 1999. These declines were much greater than those experienced in other communities, leading the study to conclude that CCTV was responsible for the difference.[26] KPMG also conducted a survey of public attitudes, finding that 79 percent agreed with the use of CCTV and 75 percent wanted the current system expanded. Also, 65 percent reported feeling that CCTV monitoring was not an invasion of privacy.[27]

b. Edmonton Police Service — The Old Strathcona Closed Circuit Television System

Edmonton's Old Strathcona Closedd Circuit Television System (OSCCTV) consisted of four cameras covering the busy shopping and bar district known as Whyte Avenue. The cameras only functioned during certain high-profile events in 2003 and 2004. While they

---

24 *Ibid.* at ix.
25 KPMG, *supra* note 19 at 1, 13.
26 *Ibid.* at 17-18.
27 *Ibid.* at 41.

were operational, the cameras were always monitored and recorded.[28] The project's official statement of purpose was to "*deter, detect, and assist in the investigation of crime* thereby decreasing the fear in, and providing a safer and less intimidating atmosphere for the public."[29] In 2005, the Edmonton Police Service (EPS) conducted an in-house evaluation of whether the OSSCTV system actually met these three goals.[30]

In terms of deterrence, the study's findings were inconclusive. The effects of CCTV could not be disentangled from various other factors, such as changes to policing tactics during the program's operation, crime prevention initiatives by the local stakeholders, and differences in the number and types of businesses in the area. Moreover, the vast majority of misconduct along Whyte Avenue consisted of spontaneous public disorder offences, often fueled by alcohol or drug consumption, and the authors cited other studies showing that CCTV has a very limited effect on this type of activity.[31]

The OSCCTV system only played a very limited role in detection. For example, the cameras ran for 544 hours during the summer of 2004. During that time, monitoring technicians only detected eleven incidents, of which only four required a police response.[32] Finally, the program did not appear to assist EPS investigations in any way. Although there were five documented requests for CCTV footage, there is no indication that it actually assisted in any investigations.[33] Since 2004, the EPS has not engaged in PVS, probably due to these inconclusive findings regarding its effectiveness and the substantial cost it involves (approximately $85,000 over the two summers).[34]

The EPS did survey public opinion prior to and during the project in 2003. Prior to the program, 75 percent of area businesses supported a permanent CCTV system, while 10 percent opposed it, and 15 percent wanted more information. A public survey showed that 39 percent approved of a permanent system, 49 percent were against it, and 17 percent indicated they were undecided. During the program's operation, a third survey found that 61 percent supported a permanent system while 30 percent were opposed and 9 percent remained undecided.[35]

This overview of the research in the U.K. and Canada indicates that it is difficult, if not impossible, to draw general conclusions about the effectiveness of PVS. To claim that it "works" or "doesn't work" is too simplistic. The effects of CCTV will vary widely depending on the system, the immediate physical environment, the larger socio-political and cultural context, the category of crime, and the defined goals of the program. Given these multiple variables, it may be impossible to predict the impact of PVS in any given situation,

---

28 Edmonton Police Service (EPS), Planning & Evaluation Services, *Review of Old Strathcona CCTV Project* (March 2005) [unpublished] at 3.

29 *Ibid.* [emphasis in original].

30 *Ibid.*

31 *Ibid.* at 3-4.

32 *Ibid.* at 4.

33 *Ibid.*

34 *Ibid.* at 5.

35 Reinhelt & Thomas, *supra* note 18 at 18.

and how that impact will change over time. The only means for assessing effectiveness would probably be to implement a pilot project, as the EPS did in 2003-2004.

B. IMPACT ON PRIVACY

The powerful image of a totalitarian state, where "Big Brother" scrutinizes our daily lives through cameras mounted on every building and street corner, is often evoked by opponents of PVS. Former federal Privacy Commissioner George Radwanski warned that, "[t]he Orwellian idea that 'Big Brother is watching' will have become no longer apocryphal, but a literal and permanent daily reality."[36] However, would police cameras aimed at public streets necessarily bring about the society described by Orwell? Or is PVS simply a neutral tactic that can be used within a liberal democracy, subject to certain controls? Before these questions can be answered, it is necessary to isolate the features of CCTV that are said to endanger privacy.

1. THE CHILLING EFFECT OF WATCHING

The "chilling effect" refers to the concept that when people feel they are continually being observed, they will consciously or unconsciously modify their behavior.[37] Former Privacy Commissioner Radwanski described this phenomenon occurring in police states:

> People know they're being watched — or worse, they're never quite sure whether they're being watched. They censor their speech and their behavior. They hurry along the streets with their heads down. They're reluctant to talk to, or even look at, any strangers.... There is very little street life or spontaneity.[38]

But does this really occur? In Canada, video surveillance has been common in semi-public spaces such as banks, stores, and malls for several decades. Customers are self-conscious when the cameras are first introduced, but soon forget that video monitoring is even taking place. People continue to attend these premises and act as freely as they would in any place where others can visually observe them. Mere "watching" by itself does not seem to account for a chilling effect. Rather, some type of negative consequence must attach to the "watching" before the behavior can be "chilled."

---

36 OPC, News Release, "Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna" (4 October 2001), online: OPC <http://www.privcom.gc.ca/media/nr-c/02_05_b_011004_e.asp>, referring to George Orwell, *1984* (London: Secker and Warburg, 1949).

37 Andrew Song, "Technology, Terrorism and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches" (2003) Berkman Center for Internet & Society, Research Publication No. 2003-04, online: The Berkman Center for Internat & Society Research Publication Series <http://cyber.law.harvard.edu/home/uploads/207/2003-04.pdf> at 14.

38 George Radwanski, Privacy Commissioner of Canada, "Video Surveillance in Public Places" (Address to the Ontario Bar Association Privacy Law Section Year End Meeting, Toronto, Ontario, 27 May 2002), online: OPC <http://www.privcom.gc.ca/speech/02_05_a_020527_e.asp>.

2. TECHNOLOGICAL ENHANCEMENTS TO "WATCHING"

Some of the chilling effect may come from a realization that cameras are more than just another set of eyes because of their technological capabilities. Video images have become sharper and clearer. The cameras themselves are smaller, and can pan and tilt. Monitors can zoom-in across great distances to read a person's newspaper over their shoulder, and can use infra-red imaging to see in the dark.[39] Digitization of video images now makes it easier to reproduce, transfer, and store the footage. Computer storage is replacing bulky videotapes, making it possible to index, catalogue, and cross-reference an enormous volume of data.[40] Digital technology also makes it easier to alter the images, leading to fears that the footage can be "doctored."[41]

Video surveillance can be combined with other technology, thereby boosting its capabilities. Facial recognition technology (FRT) is potentially the most invasive. It is a subset of biometrics, which includes retinal and fingerprint scans as well as voice identification. The technology captures a person's physical characteristic in some way, and this characteristic is then quantified. Those measurements are then compared to a database in an effort to identify the person. In the case of FRT, a video camera will record or photograph an individual's face. Computers will analyze the image, measuring spatial relationships between features such as the distance between the eyes, or the width of the nose. These numbers are then compared to a database of photos to determine if any matches exist.[42]

First generation FRT had high error rates, but the accuracy is quickly improving. The United States Department of Defense recently awarded a contract to Visionics Corporation to develop software that can recognize human faces from video at up to 35 degree angles, and that can correct for aging, facial hair, different facial expressions, glasses, and poor lighting.[43] The most famous example occurred in Tampa, Florida, where police cameras photographed some 100,000 people attending the 2001 Super Bowl game. FRT then compared the faces to a database of criminals and terrorists compiled from various law enforcement agencies, including the U.S. Federal Bureau of Investigation.[44]

In Canada, there appears to be only one example of police engaging in FRT. In 2001, the Ontario Information and Privacy Commissioner investigated reports that the Ontario Provincial Police (OPP) had secretly scanned the faces of all patrons entering casinos, and compared them to a criminal mugshot database. The Commissioner found these reports to be inaccurate. Rather, officers would only use FRT to capture a customer's facial image if they had a reasonable suspicion that he was engaged in criminal activity. That image would

---

39 Molly Smithsimon, "The Right to Privacy Is Destroyed by Video Cameras in Public Places" in Stuart A. Kallen, ed., *Are Privacy Rights Being Violated?* (Detroit: Greenhaven Press, 2006) 53 at 57.

40 Christopher S. Milligan, "Facial Recognition Technology, Video Surveillance, and Privacy" (1999) 9 S.C. Interdisciplinary L.J. 295 at 303.

41 *Ibid.* at 329-30.

42 Daniel J. Melinger, "Facial Recognition Technology Represents a Threat to Privacy" in Kallen, *supra* note 39, 64 at 65-66.

43 *Supra* note 40 at 304.

44 Rita F. Aronov, "Privacy in a Public Setting: The Constitutionality of Street Surveillance" (2004) 22 QLR 769 at 769.

then be compared to the Casino Information Database, which contains about 800 faces of known casino cheats. As a result, the OPP officers were only scanning five people for every million casino customers, and only retaining the scans if an investigation concluded that the person was committing a criminal offence.[45]

FRT thus has the potential to destroy the general public's cloak of anonymity. People might accept that as they walk along the street, various people will see them, but they take comfort in the fact that those watching do not know who they are. As Elizabeth Paton-Simpson writes,

> [a] further factor providing a degree of privacy in public places is anonymity. Often the people with whom we share public space, especially in the city or away from our usual *stamping* grounds, do not know us from the proverbial bar of soap. Any snippets of information strangers may learn from observing us are unconnected with our identities and are likely to be quickly forgotten.[46]

Some liken FRT to a police officer walking along the beat and recognizing a known criminal or just somebody he has dealt with before. But human memory is limited and gradually degrades. And the beat cop can only see so many people as he walks the streets. FRT, on the other hand, can compare hundreds of faces to a virtually unlimited database containing everything from the typical criminal mugshots, to driver's license photos, and maybe even yearbook and passport photos. Moreover, the biometric data can be matched up with other databases containing criminal records, medical information, or banking and tax records. Thus, a police officer who recognizes a person on the street might vaguely remember that he is a suspect in a bank robbery. But FRT might also reveal that the suspect has outstanding arrest warrants, that he is HIV positive, and that he has bounced a number of cheques at his bank. As Marc Blitz points out, "a pervasive and inescapable network of identification devices blurs this distinction between coincidental recognition and compelled disclosure."[47] In a sense, a person who walks in front of a camera hooked up to FRT could be potentially disclosing huge volumes of intimate information about herself without even knowing it.

3. RECORDING

For some, a characteristic of the cameras that might chill behavior is the ability to make permanent recordings. Unlike human memory, the recording will not fade with time but is potentially permanent. Emotions associated with past events also fade with memory, but can be revived upon watching the footage.[48] The permanence of the recording means that it is forever associated with the person portrayed. The freedom to escape from the consequences

---

45 Information & Privacy Commissioner of Ontario (IPC Ont.), Investigation Report, PC-010005-1: Alcohol & Gaming Commission of Ontario, "The Use of Biometric Face Recognition Technology in Ontario Casinos" (26 February 2001), online: IPC Ont. <http://www.ipc.on.ca/images/Findings/Attached_PDF/PC-010005-1.pdf> at 2-4.

46 Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U.T.L.J. 305 at 325-26.

47 Marc Jonathan Blitz, "Dangers of Fighting Terrorism with Technocommunitarianism: Constitutional Protections of Free Expression, Exploration, and Unmonitored Activity in Urban Spaces" (2005) 32 Fordham Urb. L.J. 677 at 698.

48 *Ibid.* at 695.

of past behavior is more limited when those acts are recorded for posterity.[49] As well, the footage can be played repeatedly or freeze-framed, revealing more detail than a casual glance.[50]

Recorded video also means that the potential exposure is limitless. An audience beyond the initial monitor can now view the footage.[51] And there are consequences beyond merely multiplying the number of watchers. Actions that are appropriate for one setting will often appear inappropriate when viewed outside of that situation. Video allows those actions to be exported out of their original context.[52] For example, wearing a bathing suit at a beach is completely normal. But if still footage depicting that same person in his bathing suit appears on an office bulletin board, he may be embarrassed. Moreover, when video takes those actions outside of their original context, the subject of the footage may find it difficult to justify his actions. Take the example of a store surveillance camera which records a mother spanking her child. The permanent visual image of her actions will have a greater impact with an audience than any verbal explanation she could provide after the fact.[53] As Marc Blitz states,

> [s]uch tapes also provide an objective reference point that makes it harder for a person to explain and retell an action she took by placing it in a broader context; for example, by describing it in light of motives, concerns, or other background facts that are not as vivid and uncontestable as the images captured in video.[54]

And while "a picture says more than a thousand words," it might only provide part of the story and can easily lead to incorrect inferences. A speech by former Privacy Commissioner Radwanski describes such a scenario:

> Think how easily the simple, innocent things you do can be misinterpreted by someone observing you. Someone stops you on the street and asks for directions. You tell him what he wants to know, and maybe chat for a moment. Then he goes on his way.
>
> What you don't know is that on the police screen, biometrics has identified him — rightly or wrongly — as a suspected terrorist. And, of course, your name and address are available too. The watchers have no way of knowing what was said, just that you met and talked.
>
> Next thing you know — or rather, don't know — you're in a police database as a suspect yourself.[55]

4. SYSTEMATIC SURVEILLANCE

When people go out in public, they expect their actions to be casually and intermittently observed by a number of people, including police officers. They might even expect to be

[49] *Ibid.*

[50] Paton-Simpson, *supra* note 46 at 328.

[51] *Ibid.*

[52] *Ibid.*

[53] Mitchell Gray, "Urban Surveillance and Panopticism: will we recognize the facial society?" (2003) 1 Surveillance & Society 314 at 323-24.

[54] *Supra* note 47 at 695.

[55] *Supra* note 38.

caught on camera at the local bank or store. However, a CCTV system that blankets an entire area means that the state actor can engage in systematic surveillance of an individual's every movement and action within camera range, whether illegal or not. Radwanski stated it this way:

> Clearly, we have a greater right to privacy in our homes than in public places, where we are inevitably likely to be noticed and observed by those with whom we share the space. But in those public places, we retain the privacy right of being "lost in the crowd," of going about our business without being *systematically* observed or monitored, particularly by the state.[56]

Information about one's day-to-day life would no longer be dispersed among a multitude of observers, but would be consolidated on a videotape or digital file. If the coverage area is fairly large, or a person's daily activities keep her in a particular neighborhood that is under surveillance, the police can potentially build a fairly complete picture of that person's life.

Can a police officer, following an individual from place to place, accomplish the same thing? Perhaps, but only with greater difficulty. If the officer is in uniform, the person being followed will notice and might respond with evasive action, or by confronting the officer. An undercover officer will have to take precautions to avoid being detected, making the surveillance more challenging. Generally, a team of plainclothes officers is necessary, such that police must commit significant effort and resources. These practical obstacles ensure that police will not engage in this type of surveillance lightly. Cameras, on the other hand, are usually placed at a vantage point where they can have an unobstructed view of a large area, making their surveillance more complete. It is next to impossible to know for certain whether you are being watched by video cameras perched on a roof or a pole.

5. DRAGNET SURVEILLANCE

PVS means that for the most part, cameras will indiscriminately capture innocent people engaged in completely legal activity and only occasionally detect or record illegal behavior. In other words, general surveillance engages in "dragnet" monitoring and recording, and does not proceed on the basis of any individualized suspicion or belief that those being watched have or will commit an offence. Indeed, the main goal of these CCTV systems is to cast a wide surveillance net over an area so as to deter crime before it happens. One scholar has argued that this essentially presumes that everyone is guilty until proven innocent.[57]

Police are generally required to have some form of particularized grounds — reasonable suspicion or belief — before they can detain or search somebody. Officers cannot simply decide that they are going to stop and search all individuals in a particular neighborhood, for example, in the hopes that a few of them may be carrying drugs. There are certain exceptional situations where police can search indiscriminately, such as alcohol checkstops.

---

56 *Supra* note 36 [emphasis in original].

57 Jennifer Mulhern Granholm, "Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches" (1987) 64 U. Det. L. Rev. 687 at 700.

However, those are not stand-alone searches, but arise from the detention during that checkstop.[58]

6. NOTIFICATION OF PUBLIC VIDEO SURVEILLANCE

In both the Kelowna[59] and Edmonton CCTV programs, police placed signs throughout the video-monitored area advising people of the surveillance. The EPS submitted a Privacy Impact Assessment to the Alberta Information and Privacy Commissioner, claiming that if people then walked into the area, they had implicitly consented to the camera surveillance.[60] The Commissioner disagreed.[61]

Such an argument is problematic in several respects. First, it could potentially allow the state to invade any area of privacy simply by announcing it ahead of time. Second, it is questionable whether people are actually consenting. Some will live or work in the area, and will have little choice but to walk through the monitored space. Others will object to the surveillance, but not strongly enough to stop going to their favorite coffee shop or a friend's house. Radwanski put it this way:

> People may have the choice of refusing to enter a store if there are signs warning that they are subject to video surveillance. But if there is a proliferation of surveillance cameras in our public streets, short of levitating above those cameras, people will have no way of withholding consent and still getting from place to place.[62]

7. POTENTIAL FOR ABUSE

A major concern is camera operators misusing PVS for their own gratification. A 1992 British study found that 72 percent of the respondents agreed that "these cameras could easily be abused and used by the wrong people."[63] Cameras allow the watchers to circumvent social norms in public places, such as limitations on staring, or greeting somebody you recognize to signal that there is no longer an anonymous situation.[64] Rather, cameras allow watchers to watch without being watched.

There have been several reported cases of video voyeurism. Monitors have been disciplined for zooming in on certain body parts of people they are observing, or looking into windows. Camera operators in the English Midlands used the system to take photos of

---

58 See *R. v. Hufsky*, [1988] 1 S.C.R. 621; *R. v. Mellenthin*, [1992] 3 S.C.R. 615.

59 See *supra* note 36 and *infra* note 76.

60 Sgt. Bradley W. Mandrusiak, *Privacy Impact Assessment: The Old Strathcona Closed Circuit Television Camera (OSCCTV) Project* (Edmonton Police Service, 21 March 2003) [unpublished] at 5-6.

61 Work, *infra* note 100 at para. 21.

62 *Supra* note 36.

63 Terry Honess & Elizabeth Charman, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Gloria Laycock, ed., Police Research Group, Crime Prevention Unit Series Paper No. 35 (London: Home Office Police Department, 1992), online: Home Office <http://www.homeoffice.gov.uk/rds/prgpdfs/fcpu35.pdf> at 9.

64 Paton-Simpson, *supra* note 46 at 326-27.

women with large breasts and mounted them on the walls of their control room.[65] Or, the footage may be exploited as entertainment. For example, an English film called *Caught in the Act* consisted of a montage of video clips from British CCTV systems. While it included the typical street fights, auto thefts, and robberies, it also depicted embarrassing behavior unknowingly caught on camera such as public displays of sexual intimacy.[66]

8. FUNCTION CREEP

"Function creep" refers to the usage of PVS for purposes beyond that which initially justified the surveillance.[67] Most police agencies argue for CCTV on the basis that it will deter and detect crime. However, there is growing research in the U.K. showing that camera surveillance is also targeting non-criminal but anti-social behavior such as littering, traffic violations, and even failing to plug the parking meter.[68] Here in Canada, Sudbury's Lion's Eye in the Sky project specifically targeted aggressive panhandling, public intoxication, and harassing behavior, in addition to criminal offences.[69]

Some academics claim that CCTV acts as a tool for excluding members of marginal groups from certain public or semi-public places, even when they are not engaged in criminal conduct. In commercial areas such as shopping districts or malls, camera operators have targeted "non-consumers," such as teenagers, homeless people, panhandlers and beggars, because they make legitimate customers feel uncomfortable or threatened, and may deter potential customers from frequenting the local businesses.[70]

9. DISCRIMINATORY SURVEILLANCE

A related danger to potential abuse and function creep is that PVS will target people based on their race, ethnicity, age, or apparent socio-economic status. A 1997 British evaluation by Norris and Armstrong concluded that camera monitors targeted certain groups on the belief that they were most likely to be deviant: "The gaze of the cameras does not fall equally on the users of the street but on those who are stereotypically predefined as potentially deviant, or through appearance and demeanour, are singled out by operators as unrespectable."[71] In particular, camera monitors were one-and-a-half to two-and-a-half times

---

65 Alan D. Gold, "Growth of Public Video Surveillance," News Item (15 October 2001) Alan D. Gold's Collection of Criminal Law Articles, referring to Jeffry Rosen, "A Cautionary Tale for a New Age of Surveillance" *The New York Times* (7 October 2001), online: *The New York Times* <http://www.nytimes.com/2001/10/07magazine/07/SURVEILLANCE.html>.

66 Quentin Burrows, "Scowl Because You're On Candid Camera: Privacy and Video Surveillance" (1997) 31 Val. U. L. Rev. 1079 at 1100.

67 Stephen J. Fay, "Tough on Crime, Tough on Civil Liberties: Some Negative Aspects of Britain's Wholesale Adoption of CCTV Surveillance During the 1990s" (1998) 12 Int'l Rev. L. Comp. & Tech. 315 at 326.

68 *Ibid.* at 327.

69 KPMG, *supra* note 19 at 16.

70 *Supra* note 67 at 324-25.

71 Dr. Clive Norris & Gary Armstrong, *The Unforgiving Eye: CCTV Surveillance in Public Space* (Hull: Centre for Criminology and Criminal Justice, 1997) at 6-7. For an overview of the study, see "The Usual Suspects," online: Internet Archive <http://web.archive.org/web/20010630005418/http://merlin.legend.org.uk/~brs/archive/stories 97/Suspects.htm.>.

more likely to focus on the black population then one would expect from their proportion in the general population.[72]

Indeed, the temptation to profile may be inherent in video surveillance. PVS is primarily a visual medium; few cameras have audio capability. Moreover, it is usually deployed to prevent crime, or detect it as it happens. Panning cameras across spaces might detect the odd offence in progress. But if the operators are able to predict ahead of time which persons are likely up to no good, they can focus the surveillance and possibly catch the person in the act. Obviously, this is more efficient, but the problem is that predicting who will and will not commit crimes is a very uncertain business. Camera monitors may engage in profiling based on the physical characteristics they invalidly believe indicates a "troublemaker." One would not protest if a camera operator recognized a prolific shoplifter walking through a mall, and followed him with the camera to ensure that he did not steal again. But if an operator targets individuals because of inaccurate stereotypes regarding race, ethnicity, or age, that surveillance will not only be discriminatory but also ineffective at reducing crime.

III. PRIVACY LEGISLATION

PVS must be considered in light of two types of legislation: (1) federal or provincial privacy legislation, and (2) the *Charter*. This section compares and contrasts two case studies under privacy legislation: the alleged contravention of the federal *Privacy Act*[73] by the RCMP undertaking the Kelowna CCTV project, and the adherence to the provincial *Freedom of Information and Protection of Privacy Act*[74] by the EPS with the OSCCTV.

A. THE KELOWNA CLOSED CIRCUIT TELEVISION PROJECT AND THE FEDERAL *PRIVACY ACT*

1. VIOLATION OF THE *PRIVACY ACT*

In 2001, then federal Privacy Commissioner Radwanski undertook an investigation of the RCMP's CCTV project in Kelowna at the request of British Columbia's Information and Privacy Commissioner. The federal Commissioner had jurisdiction in this case because the RCMP is a federal governmental body, even though they were contracted to provide municipal policing in Kelowna. The program consisted of a single video camera covering the downtown core in an effort to reduce criminal activity, with plans to install an additional five cameras to provide coverage of all the downtown streets. The RCMP recorded and monitored the cameras on a continuous basis, and placed signs in the area to notify people of the surveillance. In his October 2001 findings, Radwanski concluded that the project was subject to and violated the federal *Privacy Act*.[75] In April 2002, retired Supreme Court of Canada

---

72 *Ibid.* at 4.
73 R.S.C. 1985, c. P-21.
74 R.S.A. 2000, c. F-25 [*FOIP Act*].
75 *Supra* note 36.

Justice La Forest also provided the Privacy Commissioner with a legal opinion that essentially confirmed those conclusions.[76]

There was no question that at the time of the complaint, the *Privacy Act* applied to the Kelowna CCTV project. The *Act* governs the collection and use of "personal information" by governmental bodies, including the RCMP.[77] Section 3 of the *Privacy Act* defines "personal information" as "information about an identifiable individual that is *recorded* in any form."[78] Video cameras monitor individuals who can be identified. And because the cameras were recording people and their activities, the RCMP was engaged in the *collection* of information, including the physical appearance, actions, associates, and location of those "identifiable individuals."[79]

Section 4 of the *Privacy Act* only allows the collection of personal information by a government institution if it "relates directly to an operating program or activity of the institution."[80] The RCMP is in the business of crime prevention and detection, and they argued that the CCTV project would help them accomplish those objectives. But Radwanski and La Forest J. criticized this on two grounds.

The first criticism concerned the scope of information being collected. The police were not acting on the existence of specific cause as they normally do, but were recording large numbers of the general public engaged in conduct irrelevant to the RCMP's mandate. In other words, Radwanski took issue with its "dragnet" nature:

> There is no doubt that preventing or deterring crime can be regarded as an operating program or activity of the RCMP in its capacity as Kelowna's police force. But … it does not follow that monitoring and recording the activities of vast numbers of law-abiding citizens as they go about their day-to-day lives is a legitimate part of any such operating program or activity.[81]

According to Radwanski, a tenet of the *Privacy Act* is that an institution must only collect the minimum amount of personal information necessary to achieve the intended purpose. In particular, the RCMP would have to show that the collection of each piece of personal information was necessary to carry out the "operating program or activity."[82]

Nowhere is this principle of "minimal collection" explicitly stated in the *Privacy Act*, but La Forest J. agreed that this interpretation was valid in light of the *Act*'s purposes in s. 2. However, the former Supreme Court Justice indicated this might be somewhat controversial:

---

76 OPC, Opinion by Justice Gérard La Forest" (5 April 2002), online: OPC <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.

77 *Supra* note 73, s. 3.

78 *Ibid.* [emphasis added].

79 OPC, *supra* note 36.

80 *Supra* note 73, s. 4.

81 *Supra* note 36.

82 *Ibid.*

> Of course, there is no guarantee that the courts will agree with this analysis. Judges less sympathetic to privacy interests may take a more deferential approach. Some may be reluctant to read substantive, policy-based limitations into the section 4 prohibition on collecting personal information that does not directly relate "to an operating program or activity" of the institution.[83]

The second criticism considered the "effectiveness versus privacy" balance already discussed, but specifically in the context of continuous recording. On the one hand, La Forest J. claimed that permanent recordings were simply not effective. Footage might provide evidence of criminal activities that were missed by the observers, but this was unlikely if the observers monitored the cameras diligently. Recording might reduce monitoring costs, but this was not enough to justify the corresponding invasion of privacy. Moreover, recordings do not help video surveillance detect crimes as they happen; they only provide a chance to review the incident after the fact.[84] Justice La Forest seemed to place little importance on the evidence-gathering aspect of CCTV; that footage could be used to identify perpetrators after the fact, and assist in prosecution. On the other hand, the recordings themselves posed a grave danger to privacy:

> [T]he electronic recording of the movements and activities of persons by a government institution without cause threatens to obliterate the privacy interests the Act was designed to protect. This intrusion into privacy can only be justified by a compelling state interest.[85]

Prior to the release of the Privacy Commissioner's findings in October 2001, the RCMP stopped the camera recording in Kelowna, possibly in anticipation of Radwanski's conclusions, although it continued to be actively monitored. This meant that the *Privacy Act* no longer applied to the CCTV project because s. 3 defined "personal information" as *recorded* information.[86] However, Radwanski declared that while the RCMP may have satisfied the letter of the law, it had not satisfied its "spirit or intent."[87] For the former Privacy Commissioner, the only acceptable outcome was to dismantle the camera.[88]

Radwanski made repeated demands to both the RCMP Commissioner and the federal Solicitor-General to take down the camera. When they refused, the Radwanski commenced a legal challenge in the British Columbia Supreme Court. Despite his claims that the RCMP was still violating the "spirit" of the *Privacy Act*, that did not form the basis for his claim. Rather, he objected to the CCTV in Kelowna on the grounds that it violated s. 8 of the *Charter*.[89] The Court dismissed his claim, concluding that the Privacy Commissioner lacked standing to bring a *Charter* challenge. Radwanski's successor declined to appeal this finding because he did not consider it a useful expenditure of public funds.[90]

---

83 *Supra* note 76.
84 *Ibid.*
85 *Ibid.*
86 *Ibid.*
87 *Supra* note 5.
88 *Ibid.*
89 OPC, News Release, "Privacy Commissioner Launches Charter Challenge" (21 June 2002), online: OPC <http://www.privcom.gc.ca/media/nr-c/02_05_b_020621_e.asp>.
90 OPC, Media Advisory, "Charter Challenge to be Withdrawn" (4 July 2003), online: OPC <http://www.privcom.gc.ca/media/nr-c/ma_am/ma_030704_e.asp>.

2. THE FEDERAL GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE

In a speech given at various forums throughout Canada during 2002, Radwanski outlined a four-step test that police agencies needed to meet before engaging in any measure that infringes privacy, including PVS.[91] It is unclear whether he based this test on what he interpreted to be the requirements of the federal *Privacy Act*, or the *Charter*, or both. At that time, the British Columbia Supreme Court had not yet dismissed his Charter challenge. The test was as follows:

(a) *Necessity*: PVS has to be "demonstrably necessary to address a specific problem."

(b) *Effectiveness*: Police have to show that PVS is "demonstrably likely to be effective in addressing the problem."

(c) *Proportionality*: Is the harm to privacy proportional to the resulting security benefit?

(d) *Alternatives*: Police must demonstrate that other, less privacy-invasive measures, could not achieve the same result.[92]

In a speech to the Ontario Bar Association, Radwanski applied this test to a Toronto police proposal to engage in street video surveillance.[93] It was abundantly clear that in his opinion, PVS could never be justified in principle. First, there was no necessity because crime rates in Toronto and Canada had been declining for years. Radwanski did not seem to consider that there might be a more focused problem which could necessitate video surveillance in a particular neighborhood. Second, the former Commissioner claimed that all available evidence indicated that cameras on public streets did not reduce crime but merely displaced it. As discussed earlier, this is a simplistic and inaccurate generalization of the CCTV research. Third, because there were no demonstrable safety benefits, proportionality did not exist. Finally, there were many other crime prevention alternatives available, including improved street lighting, neighborhood watch programs, or increasing the number of officers on the street. However, it is unlikely that the former Privacy Commissioner inquired as to whether the Toronto police had already tried these tactics, given that he gave this same speech in several cities citing these same alternatives. Certainly, these are common problem-solving techniques that Canadian police services have engaged in for years. Radwanski therefore concluded that the Toronto proposal did not meet the four requirements of his test.[94]

In his October 2001 findings, Radwanski identified specific scenarios in which he thought police use of video surveillance would be acceptable. These included cameras to protect sensitive locations that might be vulnerable to terrorism or some other attack. It might be in response to some exceptional threat to public safety, but only if combined with other circumstances making conventional policing unfeasible. Police could also use surveillance

91 *Supra* note 38.
92 *Ibid.*
93 *Ibid.*
94 *Ibid.*

to investigate a particular crime, or engage in focused surveillance of a specific individual or individuals. However, blanket video surveillance of an entire area in response to general crime was not on his list.[95]

In March 2006, the Office of the Privacy Commissioner of Canada introduced the *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities*.[96] The Office and the RCMP developed these guidelines after an evaluation of the Kelowna project.[97] Four of the 15 guidelines appear to set a lower threshold for engaging in PVS than the test posited by Radwanski four years earlier:

(a) "Video surveillance should only be deployed to address a real, pressing, and substantial problem." Real evidence will be required to show this, and not just anecdotal evidence or speculation.

(b) Video surveillance should only be considered as an "exceptional step" to be taken in the absence of other alternatives less invasive to privacy.

(c) Police should conduct a prior assessment of the impact of the proposed video surveillance on privacy.

(d) Police should engage in public consultation prior to conducting PVS.[98]

Significantly, the guidelines do not require police to prove likely effectiveness. As previously discussed, it is very difficult, if not impossible, to predict the effects of CCTV in any specific context, and this would have been a very difficult threshold for police to meet.

These guidelines do not have the status of law but are the Privacy Commissioner's interpretation of how the *Privacy Act* applies to PVS. Essentially, the current Privacy Commissioner, Jennifer Stoddart, has given notice that the RCMP's failure to comply with these guidelines may result in her finding a violation of the *Act*. Whether the courts will agree is another matter.

---

95 *Supra* note 36.

96 OPC, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (2 March 2006), online: OPC <http://www.privcom.gc.ca/information/guide/vs_060301_e.asp>.

97 *Ibid.*

98 *Ibid.*

B. THE EDMONTON OLD STRATHCONA CLOSED CURCUIT TELEVISON PROJECT AND THE ALBERTA *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

1. ADHERENCE TO THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

Edmonton has its own municipal police service that falls under Alberta's *FOIP Act*.[99] In 2003, the provincial Information and Privacy Commissioner, Frank Work, received a complaint from a citizen about the OSCCTV cameras on Whyte Avenue. In his investigation report, Work concluded that there was no violation of the *FOIP Act*.[100]

His first finding was that the *FOIP Act* authorized the EPS to engage in this type of video surveillance. Section 1(n) defines "personal information" similarly to the federal *Act* as "recorded information about an identifiable individual."[101] "Record" is defined in s. 1(q) as "a record of information in any form and includes … images … and any other information that is … photographed."[102] Thus, video images of people constitute "personal information."

Section 33 of the *FOIP Act* states that a public body is authorized to collect personal information for listed purposes, including for the "purposes of law enforcement."[103] Section 1(h) of the *Act* defines law enforcement as follows:

> (i) policing, including criminal intelligence operations,
>
> (ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or
>
> (iii) proceedings that lead or could lead to a penalty or sanction, …[104]

Work also cited Order 2000-027, where a former Commissioner defined "policing" as "those activities carried out, under the authority of a statute, regarding the maintenance of public order, detection and prevention of crime, or the enforcement of law."[105] The EPS did indeed have this authority under the Alberta *Police Act*.[106] In particular, the stated objective of the OSCCTV program was to "deter, detect and assist in the investigation of crime, thereby decreasing the fear of crime in, and providing a safer and less intimidating atmosphere for,

---

99 *Supra* note 74.

100 Office of the Information and Privacy Commissioner of Alberta (OIPC Alta.), *Investigation Report F2003-IR-005, Edmonton Police Service, Investigation Number 2777* (6 August 2003), online: OIPC Alta <http://www.oipc.ab.ca/ims/client/upload/F2003IR005RPT.pdf> at paras. 35-38.

101 *Supra* note 74, s. 1(n).

102 *Ibid.*, s. 1(q).

103 *Ibid.*, s. 33.

104 *Ibid.*, s. 1(h).

105 *Supra* note 100 at para. 14.

106 R.S.A. 2000, c. P-17.

the public."[107] In short, s. 33 authorized the EPS to collect the personal information "in the particular circumstances pertaining to Whyte Avenue."[108]

Work found that s. 39(1)(a)of the *FOIP Act* authorized the EPS to *use* the personal information collected by the CCTV cameras. That section states that a "public body may use personal information only for the purpose for which the information was collected ... or for a use consistent with that purpose."[109] In this case, the law enforcement provision outlined in the *FOIP Act* allowed the video footage to be used for police investigations.

2. THE ALBERTA *GUIDE TO USING SURVEILLANCE CAMERAS IN PUBLIC AREAS*

Like most provinces, the Alberta government has issued guidelines for public bodies, such as the police, who engage in PVS.[110] These guidelines are similar to those set out by the Office of the Privacy Commissioner of Canada and other provincial privacy commissioners. A police agency in Alberta should consider five principles in deciding whether or not to use CCTV:

(a) Cameras should only be employed if conventional means for achieving the same goals are substantially less effective.

(b) Use of the surveillance camera must be justified by verifiable and "specific reports of incidents of crime ... safety concerns or other compelling circumstances."

(c) The benefits of surveillance must substantially outweigh the adverse effects on privacy.

(d) The agency should consult with the relevant stakeholders about the need and acceptability of the surveillance.

(e) The system should be designed and operated so that it intrudes on privacy no more than absolutely necessary to accomplish its purpose.[111]

Like the federal guidelines, the provincial guide does not have the force of law and is simply the provincial Commissioner's recommendation for complying with Part 2 of the *FOIP Act*. The Commissioner is basically warning Alberta's police services that a failure to adhere to the guideline could result in an investigation having an adverse finding. But the courts would have the final say as to whether a failure to comply with the *Guide to Using Surveillance Cameras in Public Areas* is also a violation of the *FOIP Act*.

---

107 OIPC Alta., *supra* note 100 at para. 15.
108 *Ibid.* at para. 16.
109 *Supra* note 74, s. 39(1)(a).
110 Alberta Government, *Freedom of Information and Protection of Privacy: Guide to Using Surveillance Cameras in Public Places* (Edmonton: Access and Privacy Branch, 2004).
111 *Ibid.* at 2-3.

C. A COMPARISON OF THE FEDERAL AND ALBERTA EXPERIENCES

How can we explain the different responses of the federal and provincial privacy commissioners to the Kelowna and Edmonton CCTV projects?

In Edmonton, the EPS took note of the RCMP's battle with Radwanski, the former federal Privacy Commissioner and worked to get the provincial privacy commissioner on board before starting the program. EPS lawyers submitted a Privacy Impact Assessment (PIA) to Work, along with the OSCCTV project's operational guidelines.[112] The EPS also provided statistics showing that Whyte Avenue had higher levels of "calls for service" compared to the rest of the city, especially during Canada Day.[113] PIAs are not mandatory under the *FOIP Act*, but are strongly recommended for any major project that involves the collection, use, and/or disclosure of personal information. As Work described it, the PIA is essentially a "due diligence exercise" whereby the public body evaluates whether its program will comply with the *FOIP Act*.[114] In this case, Work declared that the EPS's PIA was the first of its kind in the country and would "set the standard for police services across Canada."[115] He was also careful to state that while he had accepted the PIA, that did not equate to his approval of the project. Rather, it was an acknowledgement that the EPS had "made reasonable efforts to protect privacy, as required by the FOIP Act."[116] Thus, police agencies might forestall complications if they demonstrate to a privacy commissioner ahead of time that they have considered privacy interests.

But even if the RCMP had submitted a PIA to the federal Privacy Commissioner prior to engaging in the Kelowna program, it is highly doubtful that Radwanski would have given his approval. He voiced strong philosophical objections to PVS, making it clear that he did not believe the cameras worked and that they posed serious dangers to a free society. Subsequent to the Kelowna project, he crafted a four-step test for justifying PVS, with every indication that it would be difficult, if not impossible, for police agencies to meet those criteria.[117] For Radwanski in particular, the only option was for the RCMP to take down the cameras, and for other police agencies to not undertake PVS in the first place. However, subsequent federal and provincial commissioners might not take such a hard line. As discussed, the current federal guidelines for deciding to use CCTV do not set the threshold as high as Radwanski did in 2002. Nor does the provincial guide require police to meet such a high standard before engaging in PVS.

The objectives of the Kelowna and Edmonton programs were essentially the same: to prevent and detect crime. However, the two projects differed operationally. The RCMP program ran on a continuous basis with no delineated time frame. The Edmonton project operated for limited periods during two Canada Days and three festivals, when Whyte

---

112 See Mandrusiak, *supra* note 60.

113 OIPC Alta., *supra* note 100 at para. 5.

114 *Ibid.* at para. 3.

115 Reinelt & Thomas, *supra* note 18 at 1, quoting Frank Work after reviewing the PIA submitted by the EPS.

116 *Supra* note 100 at para. 6.

117 *Supra* note 96.

Avenue experienced larger-than-average crowds.[118] The context also differed. While both areas had higher than average offence rates, Whyte Avenue had experienced a large-scale riot on Canada Day 2001 that resulted in substantial property damage, as well as injuries to citizens and police officers. The riot attracted national media coverage and focused local attention on the problems of this particular district. Indeed, Work alluded to this incident in a postscript to his investigation report of the OSCCTV program: "I remember the repugnance I felt when I saw images of theft and vandalism on Whyte Avenue on Canada Day two years ago."[119]

A related consideration may have been that, in the aftermath of the 2001 riot, Edmonton police officers executed search warrants at media outlets in order to seize television footage of the rioters engaged in criminal offences. That footage proved essential to identifying and prosecuting many of the perpetrators. While this was not expressly mentioned in the documentation surrounding the OSCCTV program, the riot and the subsequent video evidence were probably significant considerations in the decision to undertake PVS in the area, and this may have figured in Work's decision as well. This series of events suggests that the Canada Day riot focused the purpose of the OSCCTV program in a way that did not occur with the Kelowna project.

It should also be pointed out that the EPS terminated the surveillance project on its own initiative in 2004, likely due to inconclusive findings from its own research department about the effectiveness of the cameras.[120] The service might have been hard-pressed to convince the provincial Privacy Commissioner of the need to continue or expand the project, given these preliminary findings that rated the program's effectiveness as ambiguous at best. It is quite possible that Work might have objected to the program if the EPS had tried to resurrect it in 2005 or even today.

Finally, there is a difference in the legislation. The *FOIP Act* expressly contemplates the collection of "personal information" for law enforcement purposes.[121] The *Privacy Act* has no such provision, but only provides for collection "relat[ing] *directly* to an operating program or activity of the institution."[122] The word "directly" may allow the federal Privacy Commissioner to take a narrow view of the scope of information that can be collected by the CCTV camera, which is exactly what Radwanski did. On the other hand, the express law enforcement authorization of the *FOIP Act* might make Alberta privacy commissioners more reluctant to circumscribe what information the police can collect, and instead place greater emphasis on the protection and use of that information *after* it is collected.

---

118 EPS, *supra* note 28.
119 OIPC Alta., *supra* note 100 at 8.
120 EPS, *supra* note 28.
121 *Supra* note 74, s. 33.
122 *Supra* note 73, s. 4 [emphasis added].

IV. PUBLIC VIDEO SURVEILLANCE AND SECTION 8 OF THE *CHARTER*

Section 8 of the *Charter* guarantees the right to be secure from "unreasonable search or seizure."[123] The Supreme Court of Canada set out the test for s. 8 in *Hunter v. Southam*.[124] We must first ask whether police have engaged in a "search" within the meaning of s. 8. A "search" only exists if the police action intrudes on a person's "'reasonable' expectation of privacy."[125] Second, if there is a "search," we must determine whether it is reasonable.[126]

A. DOES PUBLIC VIDEO SURVEILLANCE CONSTITUTE A "SEARCH" UNDER SECTION 8?

Former Privacy Commissioner Radwanski's legal claim against the Kelowna CCTV project appears to be the last time any party has challenged the constitutionality of PVS. The British Columbia Supreme Court dismissed Radwanski's claim on the basis that he lacked standing to bring such a challenge, and so there is still no clear answer from the courts as to whether this type of surveillance constitutes a "search" within the meaning of s. 8 of the *Charter*.[127] This is a critical problem. Police forces across Canada are spending resources on street video surveillance without knowing for certain whether the resulting evidence will ultimately be admissible in court. And, in the meantime, the constitutional privacy rights of Canadians are possibly being violated on a large scale.

Many argue that Canadians cannot enjoy a reasonable expectation of privacy in what they reveal in public. Once you step out the door of your home or office, you have chosen to expose your actions and movements to the world. But this is an American rather than Canadian viewpoint. In *Katz v. United States*, the U.S. Supreme Court famously declared that, "the Fourth Amendment protects people, not places."[128] The Supreme Court of Canada adopted this principle in *Hunter v. Southam*.[129] However, Canada's high court has not been as quick to adopt another statement made in *Katz*: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[130] Justice Dickson, writing for the Supreme Court in *Hunter*, adopted a more contextual approach:

> [A]n assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[131]

---

123 *Supra* note 3, s. 8.
124 [1984] 2 S.C.R. 145 [*Hunter*].
125 *Ibid.* at 159.
126 *Ibid.* at 159-60.
127 See *Canada (Privacy Commissioner) v. Canada (Attorney General)*, 2003 BCSC 862, 14 B.C.L.R. (4th) 359 at para. 22.
128 389 U.S. 347 (1967) at 351 [*Katz*].
129 *Supra* note 124 at 159.
130 *Supra* note 128.
131 *Supra* note 124 at 159-60.

As we shall see, current *Charter* jurisprudence does suggest that Canadians retain a reasonable expectation of privacy in what they expose in public.

Whether a court concludes that PVS engages s. 8 will necessarily depend on the nature and capabilities of the camera system, how it is operated, and how the collected footage is used. For the purposes of our discussion, it is helpful to imagine a hypothetical example at the extreme end of the spectrum: a police-operated PVS system that blankets an entire neighborhood or even a whole city, with cameras covering every block of every street, and which are monitored and recorded around-the-clock. This is the type of surveillance that evokes images of the "Big Brother" state. Would such a system survive *Charter* scrutiny?

The Supreme Court of Canada has yet to consider video surveillance in public places, but it has dealt with surreptitious video surveillance in a private place. In *R. v. Wong*, police suspected that illegal gambling was occurring in a hotel room.[132] With the hotel's consent but without judicial authorization, officers hid a video camera in the room and hooked it up to recording equipment. At trial, the accused argued that the surveillance violated his reasonable expectation of privacy pursuant to s. 8 of the *Charter*.[133]

The Supreme Court agreed. The renter enjoyed a reasonable expectation of privacy in the hotel room, even though he invited strangers in to gamble. Justice La Forest rejected the exposure principle in *Katz*, distinguishing between the risk that others may observe our activities, and that state agents will permanently record those activities on video without prior judicial authorization.[134] In particular, La Forest J. articulated the fear that unrestricted video surveillance could lead to an Orwellian state:

> [I]f a free and open society cannot brook the prospect that the agents of the state should, in the absence of judicial authorization, enjoy the right to record the words of whomever they choose, it is equally inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious video surveillance. George Orwell in his classic dystopian novel *1984* paints a grim picture of a society whose citizens had every reason to expect that their every movement was subject to electronic video surveillance. The contrast with the expectations of privacy in a free society such as our own could not be more striking. The notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society.... we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.[135]

Wong is distinguishable from PVS in three respects. First, the case dealt with focused videotaping of suspected illegal gambling. Police clearly had particularized grounds of suspicion, if not belief, that criminal activity was taking place. Second, the above statement presupposes that a reasonable expectation of privacy already existed in the hotel room and

---

132 [1990] 3 S.C.R. 36 [*Wong*].
133 *Ibid.* at 37.
134 *Ibid.* at 45-47.
135 *Ibid.* at 47.

the activities inside, whereas we cannot assume that such an expectation exists in activities occurring in public areas. Finally, the surveillance here was surreptitious, whereas street video surveillance is generally overt. Nonetheless, the above passage demonstrates the Supreme Court's concern that state video surveillance, absent judicial authorization, could lead to an Orwellian state. The Court clearly found this form of surveillance to be repugnant.

When the Court's philosophical difficulty with state video surveillance is combined with the common law treatment of other surveillance technologies, it is then possible to assess whether s. 8 will apply to the public context. In Part I.B, the features of PVS that are said to be intrusive of privacy were isolated and examined. The following section discusses the Supreme Court's analyses of those same characteristics in the context of other surveillance technologies, and how those will translate to video surveillance of public areas.

1. RECORDING AND THE CHILLING EFFECT — *R. V. DUARTE*

The recording capability of PVS has been addressed by the Supreme Court of Canada in another context: the recording of private verbal communications. In *R. v. Duarte*,[136] the Court considered whether police engage in a search when they electronically record conversations between individuals and police agents or informants who have consented to the recording. In this case, a police informant and an undercover police officer agreed to allow police to engage in audio-visual recording of their conversation with a suspected drug trafficker. Naturally, the latter party did not know about the surveillance.[137]

Justice La Forest, writing for the majority, discussed the dangers of permanent recordings:

> [I]f the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[138]

Nor did La Forest J. agree with the public exposure principle espoused by the U.S. Supreme Court in *Katz*. The speaker who confides in a listener bears the risk that the listener will repeat the information to a third party. But the speaker should not bear the risk that while he talks with the listener, the state is simultaneously eavesdropping and making a permanent electronic record of the conversation without judicial authorization. The former may be a reasonable invasion of privacy, but the latter is unreasonable.[139] This comparison translates well to the PVS context. A person who ventures out in public may bear the risk that others will see his movements and actions. But that too is completely different from the state making a permanent electronic record of that conduct.

---

136 [1990] 1 S.C.R. 30 [*Duarte*].
137 *Ibid.* at 31.
138 *Ibid.* at 44.
139 *Ibid.* at 48.

Justice La Forest made the point in *Duarte* that knowing our actions are being recorded on camera can have a chilling effect on our behavior, and quoted an American judge, Hufstedler J.: "Few of us would ever speak freely if we knew that all our words were being captured by machines for later release before an unknown and potentially hostile audience."[140] Recordings expose our words to an unintended audience, taking away our right to determine with whom we will communicate. Whether it is words or actions that are recorded, the chilling effect would theoretically be the same.

2. SYSTEMATIC SURVEILLANCE — *R. V. WISE* AND *R. V. PLANT*

In *R. v. Wise*,[141] the Supreme Court of Canada dealt with the use of an electronic tracking device to monitor the movements of the accused's car. Police suspected Wise of several murders and obtained a warrant to search his vehicle. However, officers also installed a beeper in his vehicle, which was not authorized by the search warrant, and the installation took place after its expiration. The device was a relatively crude radio transmitter that only provided the vehicle's general location, and police used it to supplement their physical surveillance. The issue before the Court was whether its installation and/or subsequent monitoring violated a reasonable expectation of privacy, such that it was a search within the meaning of s. 8.[142]

In the majority decision, Cory J. found that while people have a reasonable expectation of privacy with respect to their vehicles, it is a low one. The majority declined to distinguish between the installation and the subsequent monitoring of the beeper. Rather, the latter was merely an extension of the former.[143] Police, by installing and using the beeper, did engage in a "search." And because no prior judicial authorization was obtained as required by *Hunter*, it constituted an "unreasonable search" and therefore a violation of s. 8. The breach, however, was minor given the lower expectation of privacy in a vehicle. Justice Cory suggested that judicial authorization for such an installation could be granted on the lesser standard of reasonable suspicion.[144]

For the purposes of this article, the majority decision in *Wise* speaks to a particular feature of PVS that has been discussed: systematic surveillance. Justice Cory essentially viewed the use of the tracking device as a supplement to the police's visual surveillance of the car:

> All agree that it was quite proper for the police to physically observe the appellant and his car at all hours of the day and night. It is further agreed that these physical observations could be enhanced by the use of binoculars. Yet, it is said that the installation of this rudimentary tracking device … and the subsequent monitoring goes too far.… This I find to be a somewhat anomalous position.[145]

---

140 *Ibid.* at 50, citing *Holmes v. Burr*, 486 F.2d 55 (1973) at 72.
141 [1992] 1 S.C.R. 527 [*Wise*].
142 *Ibid.* at 528.
143 *Ibid.* at 538.
144 *Ibid.* at 538, 549.
145 *Ibid.* at 546.

In other words, if the technology helps the police conduct visual surveillance in public places, it should be allowed as long as the police obtain a search warrant on the lower grounds of reasonable suspicion.

If we apply this concept to PVS, the police may argue that they are merely using it to supplement visual surveillance. *Wise* would seem to say that this practice does violate s. 8, albeit in a minimally intrusive way. However, I would posit that general video surveillance is not meant to play a supporting role to physical surveillance. Rather, it is designed to be used on its own to potentially conduct systematic surveillance. Admittedly, the video monitor might call in police officers on the street to begin physically following the suspect. But in this case, the physical surveillance supplements the camera, and not the other way around. Where the technology essentially replaces physical surveillance, and does not merely supplement it, the courts may require a standard for judicial authorization that is higher than reasonable suspicion — in other words, reasonable and probable grounds.

However, the majority decision in *Wise* provides a shaky foundation for finding that PVS violates a reasonable expectation of privacy. First, Cory J.'s decision rests on a vehicle having a reasonable expectation of privacy. He did not address whether the accused had a reasonable expectation of privacy in his movements through public areas. Justice Cory saw the installation and subsequent monitoring as one continuous violation of s. 8. But in the case of cameras, we cannot argue that the installation itself breaches a reasonable expectation of privacy. Rather, any breach must flow from the subsequent monitoring and/or recording by those cameras.

Justice La Forest wrote a strong dissent in *Wise*, holding that a reasonable expectation of privacy does exist in one's movements through public areas. People may catch intermittent glimpses of our movements as we proceed through public spaces, but this should not justify the state's unauthorized electronic surveillance of our every move.[146] Otherwise,

> [w]e would effectively be shorn of our right to be secure against electronic surveillance the moment we left our dwellings, for a moment's reflection will confirm that as we go about our daily business many, if not the majority, of our activities are inevitably carried out in the plain view of other persons. The prospect that the agents of the state should be free, on account of this fact alone, to make it their business to electronically track all our comings and goings is simply an unthinkable prospect in a free and open society such as ours.[147]

Although the majority declined to follow La Forest J.'s reasoning, the Supreme Court has in the past embraced dissenting decisions in light of novel developments. A PVS system, depending on its scope, may indeed push a majority of the Court towards La Forest J.'s dissenting position. This is what retired La Forest J. essentially argued for in his 2002 legal opinion to Radwanski.[148]

146 *Ibid.* at 563.
147 *Ibid.* at 564-65.
148 *Supra* note 76.

A stronger basis for finding a reasonable expectation of privacy in our public movements lies in *R. v. Plant*.[149] In *Plant*, the police received an anonymous tip of a marijuana grow operation at a residential home. Without a warrant, a police officer accessed a utility company's computer database and confirmed that electricity consumption at this house was much higher than average, indicating marijuana production. The police then obtained a search warrant and found over a hundred marijuana plants. The Supreme Court dealt with whether the police's access of the database violated the occupant's reasonable expectation of privacy.[150]

The Court considered a number of factors, including the nature of the information revealed by the utility company. Section 8 only protects:

> [A] biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[151]

The majority concluded that electricity consumption did not fall within this protected sphere. However, McLachlin J.'s dissent held that utility records could reveal a significant amount of information about a person's lifestyle.[152]

Does the data captured by PVS fall within a "biographical core of information"? Hubbard, Magotiaux, and Sullivan have argued that it does not: "It is difficult to conceive how an observation of conduct *in public* could intersect with this constitutionally protected sphere of intimacy."[153] However, we live much of our lives in public, and what we display reveals a considerable amount about our personal and lifestyle choices. A police officer who catches a quick glimpse of us might derive a tidbit of information. But systematic surveillance as we move through an area can collect a greater volume and range of information, especially if we happen to live and/or work in that area. No longer is the information distributed among many different parties. The camera can see who we meet with, where we go, and which things we buy. Those isolated pieces of information can be amalgamated in the hands of the state, enabling police to create a fairly complete picture of who we are and how we live. Thus, the mere scope of the information collected by street video surveillance means that it can intrude on a "biographical core of information."

3. TECHNOLOGICAL ENHANCEMENTS — *R. V. TESSLING*

It has been demonstrated that the video camera does not merely replicate a watchful police officer. The technological enhancements inherent to video surveillance — zoom, night vision, and recording — make this analogy problematic. And the combination of video cameras with other technology, especially FRT, threatens to erase any sense of anonymity we now enjoy in public areas.

---

149 [1993] 3 S.C.R. 281 [*Plant*].
150 *Ibid.* at 281-82.
151 *Ibid.* at 293.
152 *Ibid.* at 302.
153 Hubbard, Magotiaux & Sullivan, *supra* note 20 at 224 [emphasis in original].

In *R. v. Tessling*,[154] the Supreme Court of Canada dealt with the issue of police employing advanced technology. Police, using an aircraft equipped with a Forward Looking Infra-Red (FLIR) camera, detected relative patterns of heat over the surface of a building that suggested a marijuana cultivation operation. Officers obtained a search warrant for the house based on the FLIR image and other evidence, and found a "grow-op." The issue was whether using this technology violated a reasonable expectation of privacy.[155]

The Ontario Court of Appeal had found there to be a search within the meaning of s. 8. Justice Abella wrote that, "there is an important distinction between observations that are made by the naked eye or even by the use of enhanced aids, such as binoculars, which are in common use, and observations which are the product of technology."[156] This was based on the U.S. Supreme Court's decision in *Kyllo v. United States*,[157] where the majority held that when the government uses a device "that is not in general public use" to discover details of the home which could not have been revealed without a physical search, there is a "search" under the Fourth Amendment.[158]

The Supreme Court of Canada, however, found this test of "general public use" to be ambiguous and difficult to apply. Rather, the focus should be on the nature and quality of the information revealed by the technology.[159] In other words, did the FLIR reveal any intimate details about lifestyle or information about the biographical core? Thus, when we consider the enhancements of PVS and its use in concert with other technology, the focus again has to be on what information it reveals to the monitor. Does the zoom show the contents of a letter that a person is reading? Does the FRT match the person's face with data about his buying preferences, criminal past, or his tax and income information? Because of its technological capabilities, if left unregulated PVS has the potential to intrude on the protected realm of intimate lifestyle details and core biographical data.

4. DRAGNET SURVEILLANCE — *HUNTER V. SOUTHAM* AND *R. V. THOMPSON*

It has been discussed that video surveillance of public areas is essentially a form of "dragnet surveillance." The camera will monitor scores of innocent people engaged in wholly legal activities in the hopes of spotting the odd criminal engaged in illegal activity. In *Hunter*, the Supreme Court stated that to obtain prior judicial authorization for a search, police would have to establish reasonable and probable grounds to believe that an offence has been committed and there is evidence to be found at the place of search.[160] This requirement means that police can only search on particularized grounds for specific evidence of a specific crime at a specific place. The effect is to prohibit any type of dragnet search based on indiscriminate grounds.

---

154 2004 SCC 67, [2004] 3 S.C.R. 432 [*Tessling*].
155 *Ibid.* at paras. 4-6.
156 *Ibid.* at para. 56, citing *R. v. Tessling* (2003), 63 O.R. (3d) 1 at para. 63 (C.A.).
157 533 U.S. 27 (2001) [*Kyllo*].
158 *Ibid.* at 40.
159 *Supra* note 154 at para. 58.
160 *Supra* note 124 at 168.

R. v. Thompson[161] dealt with wiretaps of public payphones. Police suspected a number of people of importing marijuana. They obtained wiretap authorizations of payphones "resorted to" by the suspects, which was permitted under the *Criminal Code*. Police installed wiretaps on certain payphones based on solid information that the suspects actually used them. But they also placed wiretaps on public telephones that just happened to be proximate to where one of the suspects was staying. On some occasions, the police officers left devices recording automatically so that the wiretaps intercepted conversations of entirely innocent and uninvolved parties.[162] The majority was particularly concerned about this privacy invasion of innocent third parties:

> [T]he extent of invasion into the privacy of these third parties is constitutionally relevant to the issue of whether there has been an "unreasonable" search or seizure. To hold otherwise would be to ignore the purpose of s. 8 of the *Charter* which is to restrain invasion of privacy within reasonable limits. A potentially massive invasion of the privacy of persons not involved in the activity being investigated cannot be ignored.[163]

Hunter and *Thompson* tell us that the dragnet nature of video surveillance does not in itself violate a reasonable expectation of privacy. Rather, if such surveillance does indeed constitute a search, its indiscriminate nature means that it could constitute an "unreasonable" search. However, it is likely that the Supreme Court would consider this dragnet quality in its decision as to whether PVS should be controlled by the s. 8 requirements in the first place.

5. CONCLUDING REMARKS

Wong provides a starting place for this analysis by illustrating the Supreme Court's philosophical objection to unauthorized state video surveillance. However, that case dealt with surreptitious video surveillance of a private place that had a reasonable expectation of privacy. It is necessary to turn to other cases where the Court has dealt with the features of PVS in the context of other technologies. Taken together, the Supreme Court's analysis of those features — recording, the chilling effect, systematic surveillance, and dragnet surveillance — indicate that PVS does violate a reasonable expectation of privacy and therefore constitutes a "search" under s. 8.

B. CAN PUBLIC VIDEO SURVEILLANCE BE A "REASONABLE SEARCH" UNDER SECTION 8?

If it is established that PVS does constitute a search within the meaning of s. 8, it must next be determined whether it can be a "reasonable" search. The Supreme Court set out three requirements for reasonableness in *R. v. Collins*: (1) the search must be authorized by law; (2) the law itself must be reasonable; and (3) police must have conducted the search in a reasonable manner.[164] This section focuses on the second requirement, but the other two require a brief discussion.

---

161 [1990] 2 S.C.R. 1111 [*Thompson*].
162 *Ibid.* at 1122-25.
163 *Ibid.* at 1143.
164 [1987] 1 S.C.R. 265 at 278.

Under the first requirement, we must ask whether PVS is authorized by either statutory or common law. As previously demonstrated, the Alberta Information and Privacy Commissioner found that Edmonton's OSCCTV program was authorized by the *FOIP Act*, but the federal Privacy Commissioner found the Kelowna CCTV project not to be authorized by the *Privacy Act*. In that event, there are two possibilities for common law authorization. One is the "plain view doctrine."[165] However, this is problematic because it requires police to have discovered the evidence inadvertently.[166] Going through the trouble of setting up a CCTV system and then monitoring the cameras can hardly be described as "inadvertent." The other common law option is the ancillary powers doctrine, whereby police have whatever powers are necessary to perform their legal duties as long as they are exercised in a justifiable way.[167] Justice La Forest suggested this possibility in his legal opinion to the Privacy Commissioner.[168]

The third requirement is that the search be conducted in a reasonable manner. Here, the privacy legislation and guidelines can offer some guidance. Police agencies should have to show necessity, proportionality, and public consultation before installing PVS. There must be operational protocols governing how the camera operators monitor and record the streets. There must also be adequate controls on the access, use, disclosure, retention, and destruction of the captured footage.

The second requirement for a "reasonable law" is more difficult. Under *Hunter*, any reasonable law authorizing a search must meet three criteria. First, there must be prior authorization. Second, that authorization must come from a neutral and impartial decision maker. Third, it must be granted on an adequate standard. In the law enforcement context, that standard will usually be reasonable and probable grounds to believe that an offence has been committed, and there is evidence of that offence to be found at the place of search. In some cases, it might be a lower standard of reasonable suspicion.[169]

This last criterion poses a seemingly insurmountable obstacle. The very purpose of PVS is to engage in generalized observation of large spaces and/or large numbers of people, in the hopes of deterring crime before it occurs or detecting crime as it happens. If police need to get judicial authorization prior to engaging in surveillance, how can they articulate what crime will be committed when, where, and by whom? How will they indicate what evidence is likely to be found by such a search? In short, the "dragnet" quality of PVS is anathema to the requirement for particularized and reasonable grounds.

A more recent case from the Supreme Court of Canada in 2003 has suggested that dragnet-type surveillance may require an even higher standard than reasonable and probable grounds. In *R. v. S.A.B.*,[170] the Court dealt with the constitutionality of the DNA warrant provisions

---

165 See *R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227.
166 *Ibid.* at para. 27.
167 See *R. v. Dedman*, [1985] 2 S.C.R. 2.
168 *Supra* note 76.
169 *Hunter*, *supra* note 124 at 160, 162, 168.
170 2003 SCC 60, [2003] 2 S.C.R. 678 [*S.A.B.*].

in the *Criminal Code*,[171] and whether the higher standard of "last resort" should be applied. This standard is employed in the context of wiretap authorizations, where judicial authorization can only be granted if the court is satisfied that other investigative techniques have been tried but failed or are unlikely to succeed. Justice Arbour held this to be unnecessary in the case of DNA warrants because they are specific to a particular suspect, whereas wiretaps are "sweeping in their reach. They invariably intrude into the privacy interests of third parties who are not targeted by the criminal investigation."[172] The implication is that because PVS widely engages the privacy interests of third parties, it would also require judicial authorization granted on the standard of (1) reasonable and probable grounds, and (2) that police have exhausted all other investigative means.

Critics thus deride PVS as inherently unconstitutional and call for the cameras to be dismantled. But PVS may be able to comply with the *Hunter* criteria[173] if the process is split into two separate phases: collection and analysis. While judicial authorization would not be required at the collection stage, it would apply at the analysis stage.

Collection would consist of automated recording, as the camera pans and tilts on a pre-determined schedule. A person may monitor the camera at the same time, but he would not interfere with its pre-determined movements unless he observed something potentially criminal. In that case, he could take manual control of the camera and engage in more prolonged, focused surveillance. But technological advances may render human monitoring unnecessary. Facial recognition technology, built into to the cameras, would allow computers to watch for known active criminals. "Behavior recognition technology" is being developed to detect suspicious movements associated to violence or the checking of vehicles.[174] For example, Bristol University in the U.K. has been developing programs that study body language to predict assaults before they actually occur.[175] Thus, if the computer detects signs of criminality, it can alert the human operator or police. Otherwise, the collection process can be completely automated.

Collection would ideally be performed by agencies independent from, or operating at arm's-length from, the police. These agencies would be subject to strict controls and audits to ensure that they are protecting the confidentiality of the information they collect. Indeed, many current CCTV systems are not under the direct control of police. In Los Angeles, California, a privately-funded community program uses civilian volunteers to monitor the cameras who then contact police if a crime is observed.[176] But with an automated PVS system, this independent agency would merely be responsible for maintaining the cameras, ensuring secure custody of the footage for a pre-determined period of time, and alerting police if the computers register a "hit."

---

171 R.S.C. 1985, c. C-46, ss 487.04-487.09.

172 *S.A.B.*, *supra* note 170 at 701.

173 *Supra* note 124 at 159-60.

174 William D. Eggers & Eve Tushnet, "Video Cameras Help Police While Protecting the Public" in Kallen, *supra* note 39, 61 at 62.

175 Helen Carter, "Eye spy" *Guardian* (1 August 2001), online: Guardian Unlimited <http://www.guardian.co.uk/Archive/Article/0,4273,4231169,00.html>.

176 Burrows, *supra* note 66 at 1105.

While the collection stage would ideally be automated and would not require judicial authorization, the analysis stage involves human access and would be judicially controlled. Analysis would include actually accessing the footage from the independent agency and viewing it, engaging in any technological enhancement such as zooming in or developing stills, subjecting the footage to any biometric technology such as FRT, marrying the video to any criminal or other type of database, or consolidating information from different cameras.

Judicial authorization could be granted on reasonable and probable grounds, or on the lower standard of reasonable suspicion, depending on how strong an expectation of privacy courts find in the collected footage. Or, the standard may vary according to the police's treatment of the footage; reasonable suspicion to only view the footage, but reasonable belief to apply FRT. The higher standard of "last resort" suggested in the *S.A.B.* case would not be necessary because at this stage, police are not engaged in a dragnet-style search that would implicate the privacy interests of scores of third parties. Rather, they are engaged in a focused search of specific evidence relating to a specific offence. And as with other search warrants, police could access the video footage without a warrant if exigent circumstances exist and they would have had the grounds to obtain judicial authorization. If police do not need the footage, it would remain locked away in a computer memory bank until it is purged after a set period of time.

Marc Blitz has proposed a similar scheme, stating that "unmonitored cameras should record everything, so that government investigators see nothing, except the minimum they need to see in order to serve the narrow mission they are charged with serving ... recordings are made automatically, but then reviewed by no one except on the basis of probable cause."[177] Washington D.C. has recently considered a variation of this type of scheme. Law enforcement can engage in warrantless video surveillance, but they would require a court order to use video surveillance with audio, zoom capability, or biometric technology.[178]

Would the collection/analysis scheme preserve CCTV's effectiveness, while minimizing its privacy-intrusive features? Theoretically, automated collection should replicate human monitoring, and be able to detect crime as it happens and provide evidence for prosecution. That in turn should deter offences before they are committed. It has been demonstrated that effectiveness will vary according to a number of factors. Yet, automated collection should not detract from whatever effectiveness a system will have.

However, the division of collection and analysis should minimize the impact on privacy. If CCTV cameras have a "chilling effect," it comes from knowing that other people are watching you, judging your actions and conduct, and telling others what you have done. But if no one will ever see the footage unless police get a warrant, that chilling effect is greatly minimized. The dangers of recording also decrease. The footage would not be preserved forever, but destroyed automatically unless required for an investigation. Nobody would ever see the video unless police can satisfy a judge that they need to. Police cannot use the cameras or the footage to engage in systematic surveillance unless they have a warrant. Nor

---

177 Marc Jonathan Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Images and Identity" (2004) 82 Tex. L. Rev. 1349 at 1467.

178 *Ibid.* at 1465.

would they be able to aggregate footage from different cameras. Dragnet surveillance of innocent Canadians would not exist because police would only access the video on the basis of reasonable, particularized grounds.

Automated collection also minimizes the potential for abuse. Human monitors would no longer be able to use the cameras for self-gratification, or to engage in discriminatory surveillance on the basis of race, ethnicity, or other protected grounds. Rather, cameras linked to biometric technology would only profile on the basis of recent criminality, which is the best predictor of future crime. Function creep would be controlled, because police would only obtain a warrant if it related to a criminal offence.

V. CONCLUSION

The British and American experiences with street CCTV strongly suggest that it will become a feature of Canadian life in the near future. Thus, there is a strong need to engage in an informed policy debate about its effectiveness and impact on privacy. Declaring that there is no evidence of effectiveness is simplistic. PVS is a complex phenomenon, and its effect on crime in any given context will be difficult to predict. Insisting that the cameras will inevitably usher in a "Big Brother" state is also misleading and alarmist. It is necessary to isolate the features of PVS that intrude on privacy, and find technological and legal means of minimizing those intrusions, rather than tearing down the cameras altogether. This article discussed how differing responses to the "effectiveness versus privacy" debate resulted in contrasting experiences under the federal *Privacy Act* and the provincial *FOIP Act*. And there is a strong basis for finding that PVS does engage s. 8 of the *Charter*. When the Supreme Court's philosophical objections with state video surveillance in *Wong* are considered alongside the Court's consideration of the privacy intrusive features of PVS in the context of other surveillance technologies, it is clear that a "search" is taking place. In that event, splitting PVS into separate phases of automated collection and human analysis is a means of ensuring that PVS will be conducted reasonably under the *Charter*.

This analysis indicates that we must move beyond the assumption underlying the "effectiveness versus privacy" policy debate. Former federal Privacy Commissioner Radwanski conceived of law enforcement and privacy interests as diametrically opposed, an approach which explains his belief that only one acceptable outcome existed: the dismantling of the CCTV camera. But the Information and Privacy Commissioner of Ontario, Ann Cavoukian, has urged Canadians to abandon this zero-sum game equation of the balancing model that suggests that public safety can only be improved at the expense of privacy, and vice versa.[179] Legal and technological solutions which allow police to engage in PVS while minimizing any adverse impact on privacy can be crafted. Privacy legislation and the *Charter* need to control the state's use of PVS, but they should not foreclose it.

---

179 Commissioner Ann Cavoukian, *National Security in a Post-9/11 World: The Rise of Surveillance ... the Demise of Privacy* (Ontario: Office of the Information & Privacy Commissioner of Ontario, May 2003), online: IPC Ont. <http://www.ipc.on.ca/images/Resources/up-nat_sec.pdf> at 48.