on aural communication techniques, and prohibits only aural, not visual, monitoring. Then, since no text explicitly refers to video monitoring, courts are free to ignore such monitoring practices, even though those practices significantly realign power relations in the workplace.

Finally, and as ever in legal tests relying on ‘reasonableness’ or ‘community standards’, there is a vicious circularity to the practice and justification of ever more invasive surveillance techniques. For example, courts have found that employees reduce or extinguish their reasonable expectation of privacy when they explicitly consent to employers’ search policies. Employers, then, demand such consent as a matter of standard business practice. That standard practice then becomes implicit in the community norms generally governing the workplace surveillance. Eventually, consent to search becomes implicit in the employment relationship. Likewise the prevalence of regulation throughout an industry can diminish privacy expectations, as can emergent public interests in, for example, security and safety.

Privacy, then, is used as a rhetorical trope more than as a guiding principle. It is sufficiently multivalent semiotically to further the various ideological ends of various legal activists. By segregating and narrowing those meanings, legal arguments around privacy have, on the whole, served to advance the power of employers vis-à-vis their employees.

Chapter 4
VIDEO SURVEILLANCE AND PRIVACY PROTECTION LAW IN CANADA

Colin J. Bennett¹, Robin M. Bayley²

4.1 INTRODUCTION: THE DEVELOPMENT OF VIDEO SURVEILLANCE PRACTICES IN CANADA

As in other industrialized states, video surveillance technologies have crept into Canadian life. Cameras have been common occurrences in high-risk private spaces such as banks, in the workplace, late-night or retail outlets where theft is prevalent, in transportation hubs (such as railway stations and airports) and in shopping malls. The familiar sign, ‘These premises are protected by video surveillance cameras’ is normally viewed without a second glance. As elsewhere, a thriving security industry has constantly pressed the case that social problems (such as theft, assault and worker inefficiency) can be addressed by more, constant monitoring. Once introduced, these technologies then raise a number of unanticipated legal, political and social questions.

However, the widespread deployment of video surveillance cameras in public places by Canadian law enforcement has generally been met with a higher level of resistance. The streets of Canadian cities, with very few exceptions, are not monitored to anything like the extent as in other countries, such as the United Kingdom. On the contrary, the few schemes for the monitoring of public places that have been proposed have generally been met with much public debate, and some considerable resistance from the community of privacy commissioners, privacy advocates and civil libertarians. As a consequence, the future of this technology in Canada as a mechanism to assist the police in the prevention and detection of crime is unclear, although it does not appear likely that Canada will be subject to the pervasive public monitoring in public places that is happening in Europe in the near future.

We should also raise a skeptical note at the outset about the difficulty of defining exactly what video surveillance technology currently means. The traditional conception is that of fixed, closed circuit television cameras (CCTV), dispersed in strategic locations and centrally recorded and monitored. But cameras are now more

¹ University of Victoria, BC, Canada.
² Linden Consulting Inc., Victoria, BC, Canada.

miniaturized, and have converged with other technologies. They can pan and zoom, provide high definition images of identifiable individuals and send the images digitally to a number of destinations. Thus, the law and policy on these issues has also to take account of devices such as webcams, wireless cams, as well as facial imaging devices. The ability to monitor is now more dispersed, mobile and intrusive.

This paper reviews the state of privacy law in Canada with respect to video surveillance technologies, broadly construed. It begins by reviewing the general state of constitutional, statutory, and civil protections, and then discusses important cases that have arisen as a result of the deployment of video surveillance cameras, and the subsequent use and disclosure of the recorded images. The law and policy on this subject originates from a variety of constitutional, statutory and common law provisions operating at both federal and provincial levels. Judgments about 'reasonable expectations of privacy' are thus not only made by the courts, but also by individual privacy commissioners, (federal and provincial) who possess a wide, but inconsistent, set of administrative and quasi-judicial powers.

4.2 The Evolution and State of Privacy Law in Canada

Canada has a federal parliamentary system of government, with responsibilities of the central or national government and those of the provinces delineated in the Constitution. Thus, there are privacy laws at both the federal and provincial level, applying to different types of organizations, depending on the Constitutional authority of the legislating government.³

The basis for the Canadian constitutional right to privacy comes from the Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982.⁴ Under the heading, Legal Rights, in ss. 7 and 8:

7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice. [and]

8. Everyone has the right to be secure against unreasonable search or seizure.

These legal rights have formed the basis of challenges to a number of state practices, and the delineation by the courts of standards for the admissibility of evidence acquired through surveillance in criminal and civil cases, for 'probable cause' as well as for the 'reasonable expectation of privacy' in public and private places. Although s. 8 is, of course, borrowed from the Fourth Amendment of the U.S. Constitution, its jurisprudence is by no means as well developed as in the United States. As we shall see, there are few Canada Supreme Court cases of relevance to the collection of personal information by means of video surveillance.

Most of the cases are therefore brought under federal and provincial privacy statutes, all of which are based on a fairly common set of information privacy principles, often termed 'Fair Information Principles'. The first privacy legislation at the federal level was contained in Part IV of the 1977 Canadian Human Rights Act, which established the office of the Privacy Commissioner, a member of the Canadian Human Rights Commission, whose main responsibilities were to receive complaints from the general public, conduct investigations and make recommendations to Parliament in an Ombudsman-type role. While Part IV succeeded in codifying fair information principles in legislation for the first time, privacy sat uneasily within a statute devoted to the question of discrimination, a related but obviously more controversial issue that tended to overshadow the importance of privacy protection.

Parallel debates over a proposed federal access to government and public sector information act in the early 1980s raised immediate questions about the compatibility between such legislation and the privacy standards within Part IV of the Human Rights Act. The current federal Privacy Act, therefore, flows from a belief that data protection should be a corollary to freedom of information, and that the various exemptions in both pieces of legislation should be internally consistent. In 1982, one Bill (C-43) incorporated an Access to Information Act and a revised Privacy Act, thus institutionalized the Canadian innovation of legislating access to information and privacy protection within the same statutory framework. This model was later copied by some of the provinces: by Quebec in 1982, by Ontario in 1988, by British Columbia in 1993, by Alberta in 1995 and by Manitoba in 1997. By the end of 2001, every Canadian province and territory had passed a legislated privacy protection policy applying to public agencies. Annex I presents the current profile of privacy protection legislation in Canada, as applied to the public sector.

The passage in 1993 of Quebec’s Bill 68, An Act Respecting the protection of personal information in the private sector,⁵ gave effect to the information privacy rights incorporated in the new Civil Code in that province, and made Quebec the first jurisdiction in North America to produce comprehensive data protection rules for the for-profit private sector. The Act applies the fair information principles to all pieces of personal information collected, held, used or distributed by enterprises engaged in an 'organized economic activity'. The Commission d'Accès à l'Information du Québec (CAI), the body established under the 1982 public sector access and privacy law, oversees its implementation, hears complaints and renders binding decisions.

After Quebec’s action, Canada became the only country in which the scope of privacy protection in one of its member jurisdictions (a province) exceeded that of the federal government. In the rest of the country, there were only a few isolated statutes relating to specific sectors, such as the consumer credit industry, and a

3 See, Barbara Melzner, Rick Shields and Kris Klein, The Law of Privacy in Canada (Scarborough: Caravan, 2000).

spreading of common law remedies and constitutional provisions of potential relevance. Throughout the decade, a number of political, international, technological and legislative developments convinced federal policy makers that this incoherent policy framework could not be allowed to continue. First, the passage of a Data Protection Directive from the European Union meant that no jurisdiction in Canada (save Quebec) could plausibly claim an 'adequate level of protection' and therefore safely process personal data transmitted from EU countries; data protection has some significant trade implications. Second, the passage of the Quebec legislation created an 'unlevel playing field' within the Canadian federation, creating uncertainties and transaction costs for businesses that operate in different provinces. Third, the publication of a series of public opinion surveys demonstrated that the general public regards privacy protection as a matter of major concern. Finally, the debates over the development and character of the Canadian 'information highway' exposed the need for a common set of 'rules of the road' for the networked and distributed computing and communications environment of the 21st century.

The result of the subsequent government commitments, policy analysis and legislative process was the Protection of Personal Information and Electronic Documents Act (introduced as Bill C-6, and now referred to as PIPEDA) which came into force on 1 January 2001. With this legislation, Canada then took a significant step towards providing a more complete set of privacy rights for its citizens. PIPEDA is based on the Canadian Standards Association's privacy standard, which contains Canada's own version of OECD privacy principles. While this law fills in some very important gaps in the existing patchwork of federal and provincial statutes that have been passed over the last thirty years or so, it does not, and cannot, regulate the entire Canadian private sector, due to the Constitutional separation of powers. On 1 January 2001 only federal works, undertaking and businesses, including the federally-regulated private sector, were obliged to comply. This includes banks, telecommunications, broadcasting, airlines, shipping and many transportation companies. PIPEDA also applies to transactions involving any company that transfers personal information across provincial or international borders in a commercial capacity.

As of January 2004, the law applies to all commercial activities of the private sector, including companies under provincial or territorial jurisdiction, unless they were covered by 'substantially similar' provincial or territorial law. Canada's Cabinet has already declared the 1993 private sector legislation in Quebec as meeting this standard. As of January 2004, only British Columbia and Alberta have passed such statutes, both called the Personal Information Protection Act. These pieces of legislation are very similar and were, in fact, developed under a common process that introduced minor provincial differences toward the end. Both statutes go further than PIPEDA in regulating personal employee information, and apply to all non-profit organizations, including unincorporated ones. British Columbia's applies both to non-profits' non-commercial and commercial activities, while Alberta's also creates a sub-category of statutorily incorporated non-profits to which PIPA only applies to their commercial activities such as selling mailing lists.

The British Columbia and Alberta statues are now in the process of being assessed by the government of Canada for 'substantial similarity'. It is expected to be only a matter of months until the substantial similarity designation process is completed, and there is little doubt that the designation will be received. In the other seven provinces and three territories, PIPEDA continues to apply to provincially regulated private businesses, including the retail sector, the manufacturing sector, some financial institutions, the private health sector, video-rental outlets, and indeed to most businesses that have face-to-face relations with consumers. Annex II presents an overview of the current state of private sector privacy legislation.

A final set of privacy laws are worthy of brief mention. In six provinces, there are statutes dating from the 1960s and 1970s which establish a tort liability for invasion of privacy. That in British Columbia, for instance, makes it a 'tort, actionable without proof of damage, for a person, willfully and without claim of right, to violate the privacy of another.'

---


7 For example: Ekos Research Associates, Privacy Revealed: The Canadian Privacy Survey (Ottawa: Ekos, 1993); Harris Louis and Alan F. Westin, The Equifax Canada Report on Consumers and Privacy in the Information Age (Ville d'Anjou: Equifax Canada, 1995); and Public Interest Advocacy Centre (PIAC), Surveying Boundaries: Canadians and their Personal Information (Ottawa: PIAC, 1995).


9 Available at <http://www.privcom.gc.ca/legislation/02_06_01_e.asp>.


11 Section 30 of PIPEDA, Transitional Provisions, prescribes its application to the provincially regulated private sector three years after PIPEDA comes into force.

12 These are available, for British Columbia at <http://www.oipc.bc.ca/private> and for Alberta at <http://www.oipc.ab.ca/pipa/act.cfm>.

13 Despite its singular status, in December 2003 Quebec instigated a Constitutional challenge to PIPEDA's provisions that make it apply to the provinces that have not passed 'substantially similar' legislation. Quebec sees this approach as an intrusion into the regulatory purview of the provinces and as setting a dangerous precedent. Depending on the outcome of this case at the Supreme Court, PIPEDA's application to provinces without 'substantially similar' legislation could be struck down.


15 (1) It is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another.

(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
4.3 CONSTITUTIONAL LAW CASES

The most influential video surveillance constitutional case is *R. v. Wong [1990]*. This case involved the video monitoring of illegal gambling activities in a Toronto hotel room on five separate occasions, and without judicial authorization by warrant. As a result of the monitoring, the police raided the room and found a large group of men, gambling paraphernalia and money. Wong and ten other individuals were accused of keeping an illegal gambling house. At the trial court level, the judge acquitted Wong, ruling that the unauthorized video surveillance violated s. 8 of the *Charter*, and that the evidence obtained should therefore be excluded under s. 24. The Ontario Court of Appeal reversed, on the grounds that Wong was running a gambling house that was open to the public, and did not have a reasonable expectation of privacy. As such there was no violation of his s. 8 Charter Rights. Wong appealed to the Supreme Court.

(3) In determining whether the act or conduct of a person is a violation of another’s privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.

(4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass'.


16 *Charter*, s. 24(2). Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

Referring to the Court’s decision in *R. v. Duarte*, a case involving the violation of the Charter’s s. 8 rights through unauthorized electronic audio surveillance, the Supreme Court first found in the *Wong* case that an unreasonable search and seizure was not dependent on the technology used. Constitutional principles should embrace all existing and future means by which agencies of the state might intrude on the privacy of the individual. Justice La Forest, writing for the majority, argued that the appropriate test was whether a person had a ‘reasonable expectation of privacy’. Traditionally, this test had been applied using risk analysis – whether or not the person being monitored had placed himself in circumstances where there was a risk of surveillance. New surreptitious technologies had, however, rendered such an approach obsolete. The more appropriate approach is to consider whether the resulting loss of freedom of privacy from unauthorized surveillance is inconsistent with the standards of privacy that people might expect in a ‘free and democratic society’.

For the majority of the court, the standards of privacy in a free and open society included the expectation of privacy behind the closed door of a hotel room. In this respect, hotel rooms should be considered no different from homes – homes away from homes. The fact that Wong invited strangers into his room for gambling did not diminish his expectation of privacy. The majority, therefore, stressed the nature of the place where the surveillance occurred, as opposed to the entire context of the behavior being monitored:

‘Clearly, our homes are places in which we will be entitled, in virtually all conceivable circumstances, to affirm that unauthorized video surveillance by the state encroaches on a reasonable expectation of privacy. It would be passing strange if the situation should be any different in hotel or motel rooms... I can see no conceivable reason why we should be shorn of our right to be secure from unreasonable searches in these locations...’

La Forest concluded that the violation could not therefore be justified under s. 24(2) of the Charter. He did, however, find that the police acted in good faith and had reasonable and probable cause to believe that a crime was being committed. The police had a ‘reasonable misunderstanding of the law’. He therefore concluded that Wong’s appeal should be dismissed, and that the evidence could be admitted in his trial.

The concurring judgments of Justices Lamer and McLachlin dissented on the question of whether the reasonable expectation of privacy should simply be as-
sessed in relation to the place where the surveillance took place. They proposed a more nuanced and contextual approach, which certainly took the place into account, but also considered the broader set of circumstances, such as the unlimited and indiscriminate invitations in public spaces to strangers to come into the hotel room: ‘A reasonable person would know that when such an invitation is extended to the public at large, one can no longer expect that strangers, including the police, will not be present in the room’. Wong did, however, affirm the principle that the fact that the accused were involved in illegal activity has no impact on their reasonable expectation of privacy.

Following Wong, subsequent cases concerning warrantless video surveillance appear to have been judged primarily on the question of whether the place being surveilled entailed a reasonable expectation of privacy, and thus whether s. 8 protections apply. In the entrance lobby of an apartment, it does not. Similarly, in the public area of a public bathroom, it does not. In the cubicle of a public washroom, whether or not the door is open, it does.

4.4 Federal Statutory Law Cases

4.4.1 The Personal Information Protection and Electronic Documents Act (PIPEDA)

The PIPEDA is the equivalent to European data protection laws. Unlike under constitutional, criminal or tort law, the individual need not be adversely affected to bring a complaint to the Privacy Commissioner of Canada. The individual need not even have ‘standing’, or be personally affected, except if the issue is in relation to a request for access to the individual’s personal information or the accuracy of that information. If it is suspected that a breach of the law has taken place, then any individual can file a complaint. The breadth of definition of personal information as ‘information about an identifiable individual’ certainly embraces the collection of an individual’s videotaped image. Unlike under the Privacy Act, see below, personal information need not be ‘recorded’ even though, under the definition of a record in the PIPEDA, the word ‘videotape’ is included.

The major issue with regard to PIPEDA is whether video surveillance constitutes an illegal collection of personal information. The central principle of the law (Schedule One Section 5(3)) ‘an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances’.

The Privacy Commissioner of Canada does not have the power to issue enforcement orders. His office investigates and then the Commissioner issues a finding, in

the form of a letter to the complainant, with a summary numbered and released for public consumption, typically without the name of complainant or respondent. Under s. 14 of the Act, an individual complainant has a right, following the Commissioner’s investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter that is referred to in the Commissioner’s report. Section 15 of the Act allows the Commissioner to apply to appear in Federal Court on behalf of any complainant to address s. 14 applications.

The Privacy Commissioner has so far reached findings in five cases (discussed chronologically below) concerning the collection or personal information by video surveillance by companies covered by the PIPEDA.

PIPEDA, Case Summary#1, 15 June 2001 (Video surveillance activities in a public place)

The first PIPEDA Finding was case #1 of 15 June 2001, and involved cameras installed by a private security firm on the top of a building in Yellowknife, Northwest Territories, aimed at the city’s main intersection below. The Commissioner, George Radwanski, found that personal information was involved, the activity was commercial (thus making PIPEDA apply), and the individuals whose personal information was captured had not consented. It is telling that this public video surveillance case is the first one the Commissioner chose to publish under the new legislation, which had come into effect at the start of the year. Later actions by the same Commissioner indicated that the proliferation of video surveillance in public places was of grave concern to him.

The complaint was initiated against Centurion Security Services by Elaine Keenan Bengts, the Privacy Commissioner of the Northwest Territories. She did not have jurisdiction because the Northwest Territories information and privacy statute applies only to the provincial public bodies and not private companies. The Privacy Commissioner of Canada’s practice is not to name either the organization or the complainant in his Findings. However, Ms. Keenan Bengts made public Mr. Radwanski’s full letter of finding, so this is a rare PIPEDA case where the participants are known.

The equipment consisted of four video cameras mounted outside with a live feed to two remote monitors in the security firm’s offices. The images were not recorded but were monitored. No audio feed was used. Staff had observed incidents and notified the police in several instances. The underlying reason for the monitoring was marketing, intended to generate business for the security firm, and this is how the activity was found to be commercial. The firm had tried to interest the City in its surveillance program, but had not elicited interest. Because the cameras generated negative publicity, the company removed them on its own volition before the Commissioner’s finding.

The Commissioner found that the company had contravened Principle 4.3 by collecting personal information without consent. He reached his conclusion that personal information was collected, not by the capability of the equipment, as in other cases cited in this paper, but because the purpose of the surveillance was to monitor people. The fact that the cameras generated live video feed, rather than tape, was considered irrelevant because the PIPEDA does not restrict its application to recorded information. This reasoning differed from the 1992 case in Sherbrooke, Quebec (see below).

Mr. Radwanski went on to explain his reasoning and general views on video surveillance:

'There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorized surveillance of public places by private sector organizations for commercial reasons. People have a right to go about their business without feeling that their actions are being systematically observed and monitored. That is the very essence of the fundamental human right to privacy, which is a crucial element of our freedom'.

The Commissioner discovered that Centurion Security Services had indicated its intention to 'pursue its efforts to provide video surveillance services to the Yellowknife community' and announced his intention to 'inform Centurion Security Services that its intended public video surveillance for commercial purposes is unlawful and cannot be pursued'. It is unclear whether the outcome would have been different if Centurion had been acting on behalf of the City or RCMP for law enforcement purposes, although the Kelowna Privacy Act case described below indicates that perhaps it would not.

PIPEDA, Case Summary #53, 28 June 2002 (Bank accused of providing police with surveillance photos of the wrong person)

While the majority of Canadian privacy cases regarding video surveillance contest the legality of videotaping as an activity in particular circumstances, other principles of fair information practices can be at issue. An example of this is the Privacy Commissioner of Canada's PIPEDA decision # 53, of 27 June 2002. It addressed a very unfortunate situation of a bank patron having been improperly identified from a bank surveillance tape as the person who cashed allegedly stolen cheques. While the complainant had been in the bank at the teller's station in question, the tape's timing roll was incorrect by 12 minutes, and she was not the person who had perpetrated the alleged crime. The victim of mistaken identity complained that the bank disclosed inaccurate personal information to police, contravening Principle 4.6 & 4.6.1.

Principle 4.6. Schedule 1, states that 'personal information must be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used'. Principle 4.6.1 states that the extent to which 'personal information must be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual'; and that information must be 'sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual'.

What makes this case so unfortunate is that two photographs of the patron's image were taken from the tape and published as the 'Crime of the Week' in the local newspaper. It is self-evident that she would have experienced embarrassment and fear for her reputation, having been publicly and erroneously identified as a criminal suspect.

The Commissioner's decision found that, given the circumstances, insufficient care was taken to ensure accuracy of information. With respect to Principle 4.6, the Commissioner had to consider how accurate the information should have been and how diligent the bank should have been about verifying accuracy. He determined as follows:

'The purpose of the information disclosure was the solving of a crime – a purpose which plainly cannot be fulfilled with wholly inaccurate information. Accuracy being crucial to the fulfillment of the purpose, the bank should have made sure that the information it disclosed was as accurate as possible'.

Considering its failure to have done so, the Commissioner found that the bank had been clearly in contravention of Principle 4.6.

In applying Principle 4.6.1, he found that the consequences of inaccurate information for the individual were such that more care should have been taken to ensure accuracy. He 'noted that an organization must take due account of the potential consequences of inaccurate information for the interests of the individual'.

'The personal information inaccurately disclosed by the bank was used to make a decision about the complainant – specifically, an erroneous decision to the effect that she was to be sought as a prime suspect in a crime.

The decision caused the complainant embarrassment and worry about her reputation and her livelihood.

Being well aware that the police would likely use the complainant's personal information to make a decision about her status as a suspect, the bank should have taken due care to ensure that the information was accurate so as to minimize the possibility of a wrong decision with adverse consequences.

Due care was by no means taken'.

In his Finding, the Commissioner noted that the bank had taken significant action to ensure the event would not occur again and that he and the individual were satisfied with the bank's action. However, they were found to be in breach of Principle 4.6.1.

PIPEDA, Case Summary #107, 19 December 2002 (Individual complains about inappropriate personal information safeguards and disclosure)

An employee of a company that supplied a railway company complained about video surveillance on the railway's premises where he made deliveries. The complaint alleged: insufficient security to safeguard personal information (not obtained by videotape); that the railway company collected his personal information by video surveillance without consent; and that the railway company had disclosed to his employer that he had made a complaint. The complaint about surveillance without consent, contrary to PIPEDA s. 5(3) and Principle 4.3, was the only basis of the complaint that is pertinent to video surveillance, and the only one discussed below.

The practice at issue was a new automated gate system which was intended to videotape the vehicle to record the condition of goods as they entered or left the facility, for limitation of liability for damages. The complainant believed that this system could record his personal information (his image) without his consent. The Commissioner found that it could, but that this collection was unintended and incidental, and was not used by the railway for any purpose. In addition, the information was retained for a short time. The Commissioner applied the reasonable person test, finding that a reasonable person would find the purpose appropriate and that consent was not necessary or appropriate.

Generalizing this case, it appears that if the purpose of the video surveillance is not to capture images of individuals (although the practice may incidentally capture such information), and the personal information is handled appropriately, then consent for the surveillance is not required.

PIPEDA Finding, Case Summary #114, 23 January 2003 (Employee objects to company’s use of digital video surveillance cameras)

In a similar case brought to the Privacy Commissioner of Canada under PIPEDA, the complainant concerned that the digital video recording cameras recently installed at a railway yard could collect the personal information of employees, specifically, their conduct and work performance, and that such information could then be used for disciplinary purposes.

Digital cameras were stationed at various places in the yard, away from work areas, and trained on areas of access. The stated purpose, of which employees were informed, was to ‘reduce vandalism and theft, liability for property damage, and minimize threats to staff safety’. The equipment involved some digital and some operational video cameras. The operational cameras could be rotated and zoomed, but did not record. Their purpose was to monitor train movements and to inform crew members of train locations. The union did not dispute the need for these cameras, and the Commissioner did not find against them, but did caution the company that using its operational camera systems for purposes other than the stated ones of efficiency and safety.

Commissioner Radwanski stated that,

'[I]n determining whether the company’s use of the digital video cameras was reasonable in this case, he found it useful to consider the following questions:

Is the measure demonstrably necessary to meet a specific need?
Is it likely to be effective in meeting that need?
Is the loss of privacy proportional to the benefit gained?
Is there a less privacy-invasive way of achieving the same end?'

PIPEDA Case Summary #131, 6 March 2003 (Citizen objects to cable company broadcasting street activities on local channel and Web site)

In case #131 of 6 March 2003, the Commissioner found that video surveillance of a street scene by the local cable station, where no identifiable images were obtained, was not personal information, and PIPEDA did not apply. This case indicates that the capability and application of the videotaping equipment should be taken into account; not merely the fact that the videotaping occurred.

The complaint alleged that the local cable company was capturing information from a camera outside its premises despite posting no notices. The information intermittently captured was distributed to the company's cable subscribers via a live-feed, and on the company's website. It was not possible to either identify license plates of vehicles or faces of individuals. The complainant was concerned that the information was available to the local police, and although the police acknowledged that they were aware of the information, it was not monitored, as it would not yield any information that could be used in a prosecution.

Although PIPEDA did not apply, the Commissioner recommended that the cable company install notices indicating that the camera could not capture personal information, to counteract the potential psychological effects from perceived privacy invasion by the public.

---

27 Available at <http://www.privcom.gc.ca/cf-de/2003/cf-de_030123_e.asp?V=Print>, PN 2004-161
4.4.2 The Federal Privacy Act

*Privacy Act*, Privacy Commissioner’s finding on video surveillance by RCMP in Kelowna, 4 October 2001

There is really only one important case involving video surveillance that has been brought under the federal *Privacy Act*, but it is perhaps the most significant and widely debated case in Canada. It arose as a result of a complaint filed by David Loukidis, the Information and Privacy Commissioner for British Columbia to the Privacy Commissioner of Canada about the installation of video surveillance equipment by the Royal Canadian Mounted Police (RCMP) in Kelowna, B.C. Most municipal police functions in large cities in Canada are performed by local forces and are under the jurisdiction of provincial law. It was only because the activity in this case was performed by the RCMP that the BC Commissioner did not have jurisdiction and was therefore left with only one means to address the situation: to raise the issue with the Privacy Commissioner of Canada.

The complaint was filed under the 1982 *Privacy Act*, s. 4 of which states that ‘no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution’. The RCMP had installed one camera purchased with funds from the City and the Downtown Kelowna Association. At the time of the complaint, the camera recorded videotape on a continual basis, 24 hours a day, seven days a week. The tapes were retained for a six-month period. The City hired four ‘watch commander assistants’ to monitor the cameras, change the tapes, and to note unusual activity.

In his finding dated 4 October 2001, the former Privacy Commissioner George Radwanski found that the camera did indeed violate the *Privacy Act*, and that therefore the complaint was well-founded. It was collecting ‘personal information’, defined under the *Privacy Act* as any ‘information about an identifiable individual that is recorded in any form’. He wrote that:

‘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. This type of wholesale monitoring or recording certainly runs afoul of the requirement to collect only the minimum amount of personal information required for the intended purpose’.

The Commissioner went on to state that this video camera was collecting personal information regardless of the existence of ‘probable cause’. Moreover, he also believed that his reasoning was consistent with the Supreme Court’s decision in *R. v. Wong* (see above), as well as with the decision of the Quebec Privacy Commissioner with respect to a similar surveillance program in Sherbrooke (see below).

He then made a variety of more general points about the purported effectiveness of video surveillance programs, about the psychological impact of having to live under conditions of constant monitoring, and about the possibility of data linkage and ‘function creep’. He also addressed the question of whether there is a ‘reasonable expectation of privacy’ in a public place, especially when there is visible and frequent notification:

‘While “reasonable expectation of privacy” is a specific legal term, what is far more important is the right to privacy. That fundamental human right cannot be extinguished simply by informing people that it is being violated. This is particularly true in the case of public space such as streets. 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 … 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’.

Before the Commissioner issued this finding, the RCMP had already ceased the practice of *recording* the video feed. The RCMP Commissioner assured the Privacy Commissioner that the area under surveillance would only be recorded if a violation of the law occurred. This put the Kelowna program technically in compliance with the letter of the *Privacy Act*, but not with its spirit. The central issue for the Privacy Commissioner was that the activities of innocent individuals (potentially identifiable) were still being monitored, even though that information was not being ‘recorded in any form’ (a stipulation that is absent from the companion PIPEDA governing the private sector). In his 2001 Annual Report, Radwanski reiterated his arguments against public video surveillance programs and expressed frustration that the RCMP had not removed its Kelowna camera, and issued a ‘solemn and urgent warning’ that the Federal Government is on a path that threatens to wipe out key privacy rights and, with them, important elements of freedom as we know it.

The Privacy Commissioner stepped up the pressure in a 15 March 2002 letter to the Solicitor General of Canada (the Canadian government Minister responsible for public safety and the RCMP). Citing ‘well-established precedent’ that when the Privacy Commissioner recommends a course of action, federal institutions comply, he asked the Solicitor-General to instruct the Commissioner of the RCMP to comply with the finding and to dismantle the Kelowna cameras. The Solicitor-General responded by suggesting that this was a provincial, rather than a federal matter. The RCMP responded by revealing plans to install a further five cameras on the streets of Kelowna.

---

29 Available at <http://www.privcom.gc.ca/cf-de/02_05_b_011004_e.asp?V=Print>, PN 2004-163.

30 <http://www.privcom.gc.ca/information/ar/02_04_10_e.asp>.
The following month, the Privacy Commissioner took the unusual step of releasing a legal opinion on the subject from the former Supreme Court Justice, Gerard La Forest (who had written the majority opinion in *Wong*). The Opinion vindicated Radwanski’s finding. La Forest wrote that “the electronic recording of the movements and activities of persons by a government institution without cause threatens to obliterate the privacy interest the (Privacy) Act was designed to protect”. He also noted that the *Criminal Code* neither authorizes nor forbids general video surveillance. Its legality must be determined by reference to the *Charter*.

With reference to the applicability of s. 8 of the *Charter* to general video surveillance, Justice La Forest made the following arguments. First, s. 8 does not rely on a rigid border between public and private domains: “Determining whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual, and fundamentally normative enterprise”. Moreover, we may have a reasonable expectation that the police will sometimes have the need to monitor our behavior in public places: “but surely it is reasonable to expect that they will not always do so”. Second, the kind of targeted surveillance practiced in the *Duarte* and *Wong* cases required a considerable investment of police time and effort. That in itself constrained the police’s ability to observe innocent individuals. General video surveillance, by contrast, allows an easier and indiscriminate surveillance of anyone within view of a camera. Thirdly, he argued that the constitutionality of video surveillance should not rest on whether or not the surveillance is recorded, as the Supreme Court has repeatedly found that unrecorded surveillance may constitute an “unreasonable search and seizure”. Finally, the constitutionality should not depend on whether or not notices are posted warning that the area may be monitored. It would make a mockery of the *Charter*; he argued, “to allow governments to extinguish a legitimate expectation of privacy by simply informing citizens that their movements and activities may be monitored”.

Thus the fundamental question is whether the investigative technique affects individual privacy to such an extent that the state agent should be expected to demonstrate probable cause before a neutral arbiter. La Forest concluded that it did. Thus, the type of general video surveillance, with or without recording, is an unreasonable search and seizure and so violates Section 8 of the *Charter*. Armed with this authoritative opinion, the Privacy Commissioner then filed a suit in the Supreme Court of British Columbia challenging the constitutionality of the Kelowna program. The Federal Government responded with a motion to dismiss the case on the grounds that the Federal Privacy Commissioner did not have standing. In March 2003, the BC Supreme Court agreed that the Commissioner’s powers of enforcement were restricted to those explicitly stated in the *Privacy Act* which does not state that he has the power to initiate proceedings in court. The question was, therefore, moot. After a highly publicized, unrelated scandal about the operation of his office, George Radwanski was forced to resign. The *Charter* case was dropped by his successor.

What distinguishes the case is neither the particular circumstances of the video surveillance, nor the decision, but instead, what happened after the Privacy Commissioner of Canada issued his findings. The various stages of the Kelowna case highlight the different attitudes toward video surveillance within the Canadian legal system and courts. Another interesting feature of the Kelowna complaint is that it was filed by the Privacy Commissioner of British Columbia. In this regard, it was similar to the Yellowknife case, despite the fact that different statutes were used. Such cases are very useful to privacy observers because they reveal the values and reasoning of more than one Commissioner. The practice of one Privacy Commissioner acting as a complainant to the Privacy Commissioner of another level of government is an artifact of the Canadian federal system of government, where an information practice that concerns a certain Commissioner may take place within the borders of his or her jurisdiction, but not be subject to the legislation that Commissioner oversees. The practice helps create a seamless fabric of privacy regulation in what could otherwise be a fragmented federal system.

### 4.5 Provincial Statutory Law Cases

Unlike the Privacy Commissioner of Canada, the provincial Information and Privacy Commissioners have enforcement powers over the public bodies within their jurisdictions. In Quebec, BC and Alberta, those commissioners now also have powers to regulate the personal information practices of businesses. To date, no video surveillance cases have arisen under these statutes. Three important cases have, however arisen in these provinces in relation to the installation of cameras by provincial agencies.

#### 4.5.1 The Quebec Act respecting access to public documents and the protection of personal information

**Final Investigation Report of Alice Lebrèque, November, 1992, File 91 07 84, La Ligue des Droits et Libertés v. La Ville de Sherbrooke**

This case was brought under Quebec’s 1982 public sector privacy legislation, the Act respecting access to public documents and the protection of personal information. The surveillance system in question was applied on Wellington Street. It consisted of four cameras in operation for about two years. Later, a fifth was added to monitor a parking lot, which had been the site of some vandalism of vehicles. The cameras were connected by secure cable to the police station. They were capable of being operated automatically, or an operator at who monitors the cameras might...
sweep horizontally and vertically and zoom in for close-ups. Images were recorded on videotape which contained images for the whole week and was re-used the following week. The tape was kept under lock and key. Two signs on the street notified citizens of the monitoring.

Investigators found that the images were small and it was virtually impossible to identify faces or license plates. Personnel were not trained to use the zoom capability. Nonetheless, the system was found to collect personal information (called ‘nominate information’, under Quebec law).

The investigation considered whether the City of Sherbrooke police had the authority to conduct the surveillance because the legislation authorizes a public body to collect information necessary to carry out its duties and implement its functions. The police were able to show a reduction in crime rate in the area of 22 per cent, although this was mostly in property crime and moving violations. Violent crime remained much the same.

The investigator considered whether the recording of data or the presence of cameras was responsible for the reduced crime. She found that only on one or two occasions was the tape consulted in an investigation. Research into surveillance cameras in Drummondville, also within the province, found that video cameras there had significantly reduced crime although none of the five cameras recorded images except when the monitoring staff detect a crime in progress. The investigator concluded that recording is not necessary for cameras to act as a deterrent. Therefore, the report concluded that the City was contravening the Act by systematically recording nominative information from the cameras. If the information is not collected and retained, the Act does not apply. It agreed that monitoring without recording is only an extension of in-person surveillance.

The City informed the CAI (the office of the Quebec privacy commissioner) that it had stopped recording images from its cameras as a result of the investigation, but intended to record when necessary (e.g., when an offence is being committed).

Ten years after this case the Quebec CAI conducted a follow-up analysis of the use of video surveillance by Quebec public agencies. They found that video surveillance was more widespread than believed: ‘66% of government agencies use surveillance cameras, mostly in places such as parking lots, garages, roads and tunnels, police stations, building entrances, stairwells, corridors, emergency exits, waiting for interview rooms, classrooms and laboratories’. The Commissioner also articulated some Minimum Rules Applying to the Use of Surveillance Cameras:

- A study of the risks and dangers as well as a crime survey, in cooperation with insurers or the police if need be, should be carried out before using cameras as surveillance tools.

- Alternatives to the use of such cameras, less invasive of privacy, should be examined. If required, such devices should be used for a limited time on limited occasions (public festivities, particular events, period of the year, hours of the day, etc.).
- The public targeted by such surveillance should be informed by any appropriate notice: information and the name, address and telephone number of the owner or user of the equipment should be provided, on a sign for instance.
- The equipment selected should only keep the necessary information, for instance: if these devices operate under someone’s immediate supervision, this person should only record pictures in case of an offence. On the other hand, in cases where continuous recording is required, the material should be kept only for a limited period.
- Surveillance cameras should never be aimed at points like: house windows, showers, bathrooms, dressing rooms, etc.
- Persons assigned to the operation of such devices should be well aware of the rules designed to protect privacy. Likewise, where outsiders are hired instead of regular employees.
- Precise rules for storing the recordings should govern the management of the information collected. Access, within the organization or the company, should be restricted.
- The rights of access and correction should be recognized to any person targeted by the recordings.
- An evaluation of the use and effects of this technology should be made regularly.

The Commissioner expected ‘scrupulous respect of the minimum rules applying to surveillance cameras’ and that ‘non-compliance with these rules could entail serious consequences’.

4.5.2 The Alberta Freedom of Information and Protection of Privacy Act (FOIP Act)

Investigation Report F2003-IR-005, Edmonton Police Service

Unlike in Quebec, the privacy protection rules for public bodies are included within more general statutes that also embrace freedom of information provisions. The

---


Information and Privacy Commissioners in provinces such as British Columbia and Alberta have 'order-making' powers; they can and do enforce the legislation by ordering public bodies to release information (personal and otherwise) in response to access requests. They also have powers to order a public body to cease or change a practice with respect to the collection, use and disclosure of personal information. Typically, however, the Commissioners have adopted more conciliatory, or mediating, strategies with the regard to the privacy-related side of their work. Two examples of the Alberta and BC Commissioners' responses to video surveillance by public bodies illustrates this different approach.

Frank Work, Q.C., Information and Privacy Commissioner of Alberta issued an investigation report on 6 August 2003 under the Alberta FOIP Act, on video surveillance by Edmonton Police Services (EPS). The investigation addressed a July 2003 pilot video surveillance program of the ‘Whyte Avenue corridor’ which was instigated after a Canada Day ‘riot’ along several blocks of Whyte Avenue on 1 July 2001. Thus the surveillance was temporary and focused on an area known for increased incidents of crime, as evidenced by statistics of increased calls for service. The Commissioner initiated the investigation after receiving a complaint after the surveillance took place.

In his report, Commissioner Work addressed compliance with the privacy provisions of the Alberta FOIP Act; the EPS’s authority to collect, use and disclose the personal information obtained by the surveillance; the retention of the personal information; and the reasonableness of the security arrangements. The Commissioner concluded that the EPS had not been diligent in justifying the need for surveillance and developing policies and procedures to address the collection, use, disclosure, security, correction and retention issues. He concluded that, as long as the video surveillance was carried out, and the personal information handled as described in the PIA, the video surveillance was in compliance with the FOIP Act.

One of the significant aspects of this case was the preparation of a Privacy Impact Assessment (PIA) by the EPS, even though this was not required under the law. In a postscript to the report, the Commissioner took the opportunity to comment on larger issues. He complimented the EPS on its PIA, which he described as ‘well-done’ and ‘sensitive to the civil liberty issue’ insofar as cameras would only be operated during the periods of highest risk and under strict conditions’, thus sending the message that his investigation report did not open the floodgates for indiscriminate public video surveillance in Alberta. Mr. Work also mentioned that while the PIA is not required by the FOIP Act, it is a useful tool and one that it ‘made the special case for cameras on parts of Whyte Avenue as a law enforcement tool’ in this instance. He further stated that ‘[s]urveillance cameras and general public surveillance must not be seen as the common solution to every crime or security problem’. He observed that a number of measures had contributed to the ‘riot’, and that surveillance alone was not likely to prevent its recurrence.

This Investigation Report is described as ‘the formal, legal conclusion to the process’. However, either party can request that the Commissioner hold a formal Inquiry, resulting in a binding Order. Orders may be judicially reviewed.

4.5.3 The British Columbia Freedom of Information and Protection of Privacy Act

Investigation Report P98-012: Video Surveillance by Public Bodies: A Discussion

A somewhat different approach was adopted by the British Columbia Commissioner, David Flaherty in 1998. Although this investigation was not the result of a complaint, it also did not result in a binding Order. The Commissioner instigated the investigation after several routine site visits to hospitals, correctional facilities, police departments and the organizations that were the direct subjects of the investigation, the Vancouver Public Library and the Headquarters of the Insurance Corporation of British Columbia (ICBC).

Rather than producing a more specific report, as with the case of the Edmonton Police Department above, he decided instead to issue some more general Guidelines on Video Surveillance by Public Bodies, citing the Vancouver Library and ICBC as ‘case studies’. This approach reflected the Commissioner’s ‘pragmatic’ attitude to privacy issues:

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

Some of the key guidelines of the report are as follows:

- Public bodies should have a formal, written policy on video surveillance and ensure employees and contractors are aware of it and apply it. They also should ensure that members of the public are aware of any video surveillance in operation at their offices by posting highly-visible notices.
- Public bodies should carefully choose sites for camera installation so that their placement is restricted to identifiable areas. They should conduct video surveillance only where surveillance is necessary and is a viable deterrent. Cameras should not be placed where the public has a reasonable expectation of privacy (e.g., washrooms and change rooms).

35 <http://www.oipc.bc.ca/investigations/reports/invrpt12.html>
36 <http://www.oipc.bc.ca/new/rlsinvg/rlsinvg12.html>
Public bodies should restrict use of video surveillance to identifiable time periods when there is a higher likelihood of incidents in the particular vicinity.

Public bodies should appoint an internal review officer to audit the use and security of surveillance cameras, including monitors and tapes. All camera operators should be aware that their camera operations are subject to audit and that they may be called upon to justify their surveillance interest in a particular employee or member of the public.

A recorded videotape is a record under the Freedom of Information and Protection of Privacy Act and is therefore subject to the Act’s fair information practices with respect to the collection, use, and disclosure of personal information. Under the Act, public bodies may collect personal information on videotape to detect or deter criminal offences which occur in view of the cameras, or for inquiries and proceedings relating to law enforcement or research. Public bodies may not use video surveillance for other purposes, unless expressly authorized by, or under, other legislation.

An individual who is the subject of video surveillance by a public body has a right under the Freedom of Information and Protection of Privacy Act to request access to the videotape. However, an individual may receive only partial access to the tape if certain portions must be severed under the Act, such as to protect the personal privacy of other individuals.

The report concluded:

‘I strongly encourage all public bodies that use video surveillance to comply with the recommendations of this Investigation Report. I have found that the use of video surveillance by public bodies is justified only if such information collection is both necessary under s. 26 of the Act and follows the fair information practices outlined in this Investigation Report’.

It is interesting that these ‘Guidelines’ are described as ‘recommendations’. By following these recommendations, public bodies in BC are given the clear message that this is the only way that they can conduct video surveillance operations and be in compliance with the law. While these policy instruments are not binding, the Commissioner and his staff will use them in assessing any public video surveillance practice that is subject to a complaint, and it is a public message about their attitude toward video surveillance. By issuing an Investigation Report, the Commissioner stopped short of issuing an order, which he certainly has the power to do. Instead he relied on a more subtle and conciliatory approach, designed in the long run to achieve a higher level of compliance.

In January, 2001, the next Commissioner, David Loukidelis, updated these guidelines, ‘to assist public bodies in deciding whether collection of personal information by means of a video, audio or other mechanical or electronic surveillance system is both lawful and justifiable as a policy choice and, if so, how privacy protection measures should be built into the system’. The Ontario Commissioner has followed with both general guidelines, and more specific advice for the installation of cameras in schools. What remains to be seen is whether provincial commissioner will apply these guidelines, as is, to cases involving video surveillance by the private sector under the new private sector data protection laws.

4.6 Provincial Civil Law Cases

The administration of the civil law in Canada is an exclusively provincial responsibility. The existence of provincial privacy tort laws provides opportunities for a range of possible claims between private parties when video cameras are being used in an allegedly intrusive manner. The vast majority of these cases have occurred in an employment context between insured and insurers, and employers and employees, both at and off the work site. But the use of cameras in the workplace is not a new development. Thus the law on video surveillance builds upon a series of provincial cases about the permissibility of monitoring employees for the purposes of deterring theft, improving efficiencies, the abuse of sick leave privileges, the detection of fraudulent claims for disability insurance, and compliance with laws and standards (such as health and safety regulations). The state of the law is impossible to summarize. Two cases, one in Quebec and one in British Columbia, both signal the difficulty of relying on privacy claims, especially against powerful corporate interests.

Le syndicat des travailleurs(euses) de Bridgestone-Firestone de Joliette (CSN) v. Me Gilles Trudeau et Bridgestone/Firestone Canada Inc.

Video surveillance of daily activities has become an effective and sometimes conclusive means for verifying the good faith of an insured who has filed a claim for

---


41 C.M., 500-09-001456-953, 30 August 1999, Justices LeBel, Baudouin and Thibault. This case is only in French and has been summarized from Jean Saint-Onge In Fact And In Law, Life and Disability Insurance Law, September 1999, at <http://www.laverydebilly.com/pdf/bulletins/990903a.pdf>.
disability insurance. In this case, an employee fell at work, and consulted a doctor who provided him with a certificate for sick leave. A few days later, the employee saw the company's nurse who did not notice any evidence of the condition that he was claiming (a contusion of the hip). The company doctor found that he was fit for work. The employee did not return. Suspecting fraud, the company hired a private investigator who instigated three separate daily surveillance programs, each of which revealed the employee going about normal daily activities without evidence of back or hip pain. He was confronted by management who dismissed him for having lied about his physical condition in order to extend the period of disability.

The case eventually reached the Quebec Court of Appeal. As this was a case of private dealings between an employee and his employer (and by extension his insurance company), the Canadian Charter of Rights and Freedoms did not apply. The court relied on the Quebec Charter of Human Rights and Freedoms, as well as the provisions of the Civil Code of Quebec, Article 36 which prohibits surveillance on invasion of privacy grounds. Any violation of the right to privacy, outside the workplace, had only been permitted under precise and exceptional circumstances.

The Quebec Court of Appeal decided in this case that the surveillance was justified. Under the tests applied in the Bridgestone/Firestone case, surveillance of employees can only occur if it satisfies the following criteria:

- There must be a link between the measure taken by the employer and what is necessary for the proper operation of the business;
- The decision to put the employee under surveillance must not be arbitrary;
- The employer must have serious grounds to question the employee’s honesty before putting him under surveillance;
- The surveillance must appear necessary in order to verify the employee’s behavior;
- The surveillance must be carried out with as little intrusion as possible.

By filing a work related claim, therefore, the employee had effectively waived his right to privacy and invited an appropriate investigation to take place.

Richardson v. Davis Wire Industries Ltd. 42

Most cases concerning the video taping of employee behavior in provinces outside Quebec are ruled on by labour arbitrators in the context of existing collective agreements between employers and unions. 43 This 1997 case actually reached the Supreme Court of British Columbia. Richardson was a long-term employee serving as a production supervisor at Davis Wire Industries Ltd. Employees reported to the employer that Richardson was sleeping on the job during night shifts in the cafeteria. The employer installed a recording video surveillance camera which operated for several nights. The tapes appeared to show Richardson sleeping, so the General Manager entered the lunchroom on a subsequent night shift to confront Richardson, who was startled awake. According to his supervisor, Richardson lied about his history of sleeping on the job, and was dismissed for abusing a position of trust.

One of five issues for the Supreme Court of British Columbia was whether the video tape evidence presented at trial was admissible. The videotaped evidence was important for establishing whether Richardson lied, because sleeping when he was not on breaks was not necessarily, of itself reason for dismissal. Richardson’s defense was based on an argument that the surveillance violated his right to privacy under the provincial Privacy Act, R.S.B.C. 1979, c. 336. His counsel asserted that the right to privacy must be weighed against the company’s right to investigate. Relevant considerations include the reasonableness of requesting surveillance, the reasonableness of the surveillance itself, and other alternatives open to the company to obtain the evidence it sought. She contended that Richardson expected a high degree of privacy in the foreman’s lunch room.

The court concluded, however, that there was no expectation of privacy on the part of Richardson in the circumstances. Furthermore, even if he had an expectation of privacy, a breach of privacy does not lead to exclusion of the evidence in this case. The British Columbia Privacy Act merely provides the foundation for a claim in tort and does not prohibit the admission of evidence, even if it were gathered contrary to the Act. ‘Richardson could not reasonably expect to have the protection of privacy when he was sleeping on company time, on company property, and in circumstances where he could be expected to be contacted if needed’, the court concluded.

However, the Court expressed regret that the employer chose to install the surveillance equipment. ‘In my opinion’, Justice P.A. Kirkpatrick, wrote, ‘the surveillance of an employee in hopes of catching him or her engaging in a type of wrongdoing … is itself a practice which jeopardizes the relationship of trust and confidence that is so crucial to the employer/employee relationship’. She opined that it might have been better for the employer to have simply confronted the employee about his misconduct before resorting to video surveillance.

4.7 Conclusion

From the foregoing review, we can reach a number of conclusions about the state of the law on video surveillance in Canada. There is no question that this is one of the most significant privacy issues facing Canadian citizens. Video cameras provide a direct and visible manifestation of surveillance, raising the specter of ‘Big Brother’ and the deep concerns of privacy advocates, privacy regulators and the public at

large. As a result, the wholesale introduction of video surveillance in Canadian cities has been, at least partially, resisted. As the Kelowna case demonstrated, its constitutionality under the Charter is still unsettled.

The sources of law on video surveillance in Canada are multiple. Permissible standards have been articulated by the federal courts, by provincial courts, by the federal Privacy Commissioner, by provincial Information and Privacy Commissioners, as well as by labour arbitrators. The applicable law may be constitutional (federal and provincial), data protection regulation (federal and provincial) and civil (provincial). A number of 'quasi-legal' instruments (particularly the 'Guidelines' issued by provincial commissioners) are also of considerable importance. Despite this diversity of legal authorities, it does appear that the standards for the deployment of video cameras have been converging and becoming more precise - at least with regard to public agencies.

The primary constitutional test concerns the existence of a 'reasonable expectation of privacy' on the part of the person being monitored. That still depends principally on an uneasy distinction between public and private places. For statutory law, there is little question that the information collected via video surveillance constitutes 'personal information' under both federal and provincial statutes, provided that the images are sufficiently clear potentially to permit identification. Under the federal Privacy Act, however, it appears that the surveillance does need to be recorded, and not simply collected. With the exception of the former Privacy Commissioner, George Radwanski, the other commissioners have chosen not to try to impose a rigid consent standard to the collection of personal information via video surveillance. Each has adopted a more pragmatic approach to this technology, preferring to manage its worst effects rather than to prevent its deployment per se.

As a result, the provincial commissioners have drawn lessons from one another and have each drawn up quite similar policies, based on the following conditions:

- Has a need been established?
- Have alternatives to video surveillance been considered?
- Is there an internal written policy, overseen by a responsible officer?
- Is the placement of the cameras restricted to the most narrow focus?
- Are the cameras operational only during the most necessary time periods?
- Is there adequate notification that the area is being monitored?
- Are there appropriate security procedures for the tapes?
- Are there effective rules for the prohibition of unauthorized access to recorded images?
- Are there clear rules for the retention of tapes?
- Are rights of access and correction afforded?
- Has a risk analysis been completed, in the form of a Privacy Impact Assessment?

With respect to provincial public agencies, at least, standards do appear to be converging. We might expect to see similar rules emerge as a result of the cumulative findings under the federal PIPEDA.

Whether or not these standards will stand the test of time, on the other hand, is very much an open question. New, more surreptitious, mobile and miniaturized image capturing devices have recently entered Canadian life, and are putting the tools of the private investigator directly into the hands of individuals. These products might be advertised for a number of quite beneficial purposes: watching children's browsing behaviour, monitoring child care centers and seniors' nursing homes, enhancing home security, keeping an eye on contractors, babysitters and so on. The product manufacturers sometimes cannot resist, however, touting other possible uses for the web cameras whose legitimacy may be more questionable, and rarely point out that the monitoring of employees such as babysitters and contractors without their knowledge and consent might be illegal in some jurisdictions.

These, and other products, are radically altering the conception that we have of 'video surveillance'. Most of the cases mentioned in this paper involve fairly traditional monitoring by fixed cameras. Few involved wireless or web-based devices. None involved the matching of the images with digital facial-imaging software. With this in mind, despite the successes, the above account of the law and policy on video surveillance in Canada seems also to be a familiar story of public policy responses striving to catch up with rapidly evolving technological developments.

---

### Annex I
STATUS OF PUBLIC SECTOR PRIVACY LEGISLATION IN CANADA

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Name of Act</th>
<th>Date proclaimed</th>
<th>Oversight Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Privacy Act</td>
<td>1982</td>
<td>Privacy Commissioner of Canada</td>
</tr>
<tr>
<td>Manitoba</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1997</td>
<td>Office of the Manitoba Ombudsman</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>Protection of Personal Information Act</td>
<td>2000</td>
<td>Office of the Ombudsman</td>
</tr>
<tr>
<td>Newfoundland</td>
<td>Privacy Act</td>
<td>1996</td>
<td>Director of Legal Services</td>
</tr>
<tr>
<td>Ontario</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1988</td>
<td>Information and Privacy Commissioner/Ontario</td>
</tr>
<tr>
<td>Prince Edward Island</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>2001</td>
<td>Assistant Clerk of the Committee Legislative Assembly</td>
</tr>
<tr>
<td>Quebec</td>
<td>An act respecting access to documents held by public bodies and the protection of personal information</td>
<td>1982</td>
<td>La Commission d'Acces à L'Information du Quebec</td>
</tr>
<tr>
<td>Saskatchewan</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1992</td>
<td>Information, Privacy and Conflict Of Interest Commissioner</td>
</tr>
<tr>
<td>North West Territories/Nunavut</td>
<td>Access to Information and Protection of Privacy Act</td>
<td>1996</td>
<td>Information and Privacy Commissioner</td>
</tr>
<tr>
<td>Yukon Territory</td>
<td>Access to Information and Protection of Privacy Act</td>
<td>1996</td>
<td>Office of the Ombudsman</td>
</tr>
</tbody>
</table>

### Annex II
STATUS OF GENERAL PRIVACY PROTECTION LAW FOR THE PRIVATE SECTOR

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Act or other official action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Protection of Personal Information and Electronic Documents Act</td>
<td>2001</td>
</tr>
<tr>
<td>Alberta</td>
<td>Bill 44, The Personal Information Protection Act</td>
<td>2003</td>
</tr>
<tr>
<td>British Columbia</td>
<td>Bill 38 “The Personal Information Protection Act”</td>
<td>2003</td>
</tr>
<tr>
<td>Manitoba</td>
<td>Discussion Document Published</td>
<td>1999</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>Discussion Document Published</td>
<td>1998</td>
</tr>
<tr>
<td>Newfoundland</td>
<td>No known official action</td>
<td></td>
</tr>
<tr>
<td>Nova Scotia</td>
<td>No known official action</td>
<td></td>
</tr>
<tr>
<td>Ontario</td>
<td>Discussion document published. Bill introduced and withdrawn</td>
<td>2002</td>
</tr>
<tr>
<td>Prince Edward Island</td>
<td>No known action</td>
<td></td>
</tr>
<tr>
<td>Quebec</td>
<td>Bill C-68 (An Act respecting the Protection of Personal Information in the Private Sector)</td>
<td>1993 (amended 2001)</td>
</tr>
<tr>
<td>Saskatchewan</td>
<td>Internal consultations</td>
<td></td>
</tr>
<tr>
<td>North West Territories/Nunavut</td>
<td>Access to Information and Protection of Privacy Act</td>
<td></td>
</tr>
<tr>
<td>Yukon</td>
<td>No known action</td>
<td></td>
</tr>
</tbody>
</table>