COMPUTER AND E-MAIL WORKPLACE SURVEILLANCE IN CANADA: THE SHIFT FROM REASONABLE EXPECTATION OF PRIVACY TO REASONABLE SURVEILLANCE

Professor Michael Geist*
University of Ottawa, Faculty of Law
Director of E-commerce Law, Goodmans LLP

March 2002

Prepared for: Canadian Judicial Council

Table of Contents

> "Surveillance technology is neither inherently bad nor good, but…there is both good and bad surveillance."
>
> - David Flaherty, B.C. Information and Privacy Commissioner, Investigation P98-012[1]

Surveillance in society is not a new issue. In years past, Orwellian visions of video cameras on every street corner and wiretaps on every telephone left many fearful of a world without personal privacy. Although audio and video surveillance worries have not disappeared, the ubiquity of computing and Internet communications has catapulted computer and e-mail surveillance to the forefront of public attention. This attention is particularly pronounced in the workplace, where millions of computer-enabled employees who are familiar with their word processing and e-mail applications, may know little about surveillance technologies that quietly monitor their network activity or even worse, their every keystroke.

Companies of all sizes have begun to install computer surveillance technologies that specifically target employee use of information resources. Up to 14 million workers in the United States alone have their e-mail and Internet use monitored.[2] A 2001 survey by the American Management Association (AMA) revealed that nearly 80 percent of major U.S. companies monitor employee e-mail and Internet use, a dramatic increase from the 35 percent of companies identified in 1997.[3] Of particular note was the fact that, "[i]n previous years the growth in monitoring went hand in hand with increases in the share of employees gaining access to e-mail and the Internet. This year, however, the average share of employees with office connections showed little growth, while monitoring those activities rose by nearly 10 percent."[4] Similarly, a study by the Society for Human Resource Management found that 74 percent of the 722 companies surveyed said that they monitored workers' Internet use and 72 percent said they checked on employees' e-mail.[5]

Moreover, computer surveillance is not limited to the mainstream workplace. The Judicial Conference of the United States, the body that determines how the judicial branch in that country administers itself, created a wave of controversy in 2001 after

it recommended wide-scale monitoring of all computers used by the judiciary and their staff.[6] The recommendation touched off a storm of protest from senior judges across the country, with the 9th Circuit judiciary voting unanimously in the spring to disable the monitoring software.[7] The matter was resolved several months later when a modified proposal was adopted.[8]

Similar concerns arose in New Zealand in early 2002 after reports surfaced that several judges had accessed pornographic Web sites from their workplace computers.[9] The information came to light following a routine audit of Internet access records, a practice provided for by the New Zealand Department of Courts' computer use policy.[10] Although none of the content accessed was illegal, the revelations garnered national headlines that were accompanied by calls for the resignations of the implicated judges.[11] An immediate investigation revealed that all but one judge had accessed the content accidentally or for work-related purposes.[12] The last judge was subsequently cleared of any illegality, though calls for his resignation persisted in the scandal's aftermath.[13]

While computer surveillance of the judiciary raises particularly complex considerations, the legal issues that accompany computer surveillance in the traditional workplace are often misunderstood. Many people assume that employers' ownership of the computing equipment and the right to set workplace rules grant them an unfettered right to monitor employees' computer usage provided that they disclose the practice. A close examination of relevant statutes, case law, and policy releases from leading privacy agencies reveals that the matter is open to debate, however, particularly when the United States' approach is contrasted with that in Canada. Many cases and comments suggest that while notice is indeed a necessary pre-condition to most forms of computer surveillance, notice alone is rarely sufficient to support the practice.

This paper examines the issue of computer and e-mail surveillance from a

Canadian legal perspective with specific focus on surveillance within the judiciary. Part one provides background on current computer and e-mail monitoring practices. It examines the primary rationales companies provide for installing surveillance technologies and provides an environmental scan of the leading technologies presently available on the marketplace.

Part two canvasses the legal approaches to computer surveillance in Canada. Following a brief review of leading U.S. jurisprudence, the paper considers the sizable number of Canadian statutes that place a premium on privacy considerations. Case law from both Canadian courts and administrative panels are also examined, as is the policy position of Canada's Privacy Commissioner, who is charged with the responsibility of administering Canada's two leading privacy statutes. This portion of the paper concludes that the legality of computer surveillance in Canada is gradually shifting from an analysis of the target's reasonable expectation of privacy to an assessment of the reasonableness of the computer surveillance. This assessment comes as courts and policy makers seek to strike a balance between employers' legitimate workplace concerns that support surveillance initiatives on the one hand and employees' right to privacy on the other.

Since determining the reasonableness of surveillance can be a highly subjective exercise, part three proposes six factors that should be considered in the assessment. The six factors, which may differ in importance under varying circumstances, include (i) the target of the surveillance, (ii) the purpose of the surveillance, (iii) the prior use of alternatives to computer surveillance, (iv) the type of technology used to conduct the surveillance, (v) the adequacy of the notice provided to the target of the surveillance, and (vi) the protection of other privacy norms, such as privacy administration, security, and data retention, once the surveillance data has been obtained.

Part four applies the reasonableness criteria to prospective computer

surveillance of the judiciary. The controversy over judicial computer surveillance in the United States and New Zealand highlighted the potential for surveillance to compromise the protections afforded to the judiciary to ensure its judicial independence. From a Canadian perspective, case law supports the necessity for judicial immunity as a pre-condition for liberty and certain forms of computer surveillance within the Canadian judicial branch could place that immunity in jeopardy.

Part One – Computer Surveillance in the Workplace: The Why And How

a. Why Companies Deploy Computer Surveillance Technology

With nearly 80 percent of major U.S. companies now monitoring employee e-mail and computer usage,[14] it is worth considering why so many organizations are willing to invest in such technologies. Although the relatively inexpensive cost of surveillance technologies (particularly when calculated as a percentage of overall information technology expenditures) is unquestionably a factor,[15] companies point to several other rationales, many legal in nature, as the prime motivators behind installing surveillance systems in the workplace environment.

i. Employee Productivity

As companies install ever-faster personal computers on the desktops of millions of employees, concerns over employees' personal use of computing resources has emerged as a major issue. In fact, in one recent study, over 75 percent of companies said that monitoring their employees had helped them fight personal use of the Internet during business hours.[16] Another survey revealed that "the majority of employees spend anywhere from 10 minutes to an hour every work day surfing sites unrelated to doing their jobs -- using their work computers to read virtual newspapers, shop for clothes, or observe naked women."[17] The survey further reported that 25 percent

of employees said they spent 10 to 30 minutes a day at work surfing non-related work sites. Twenty-two percent said they spent 30 minutes to an hour; 12 percent said they spent one to two hours; while 13 percent admitted to spending more than two hours a day online at sites unrelated to their jobs.[18]

Canadian data has uncovered similar trends. A poll conducted by the Angus Reid Group in 2000 concluded that Canadian employees waste nearly 800 million work hours each year surfing the Internet for personal reasons.[19] The poll also found that Canadians with Internet access at work spend an average of eight hours online a week, and of that, at least two hours is for personal reasons.[20]

ii. Network Performance

Closely related to employee productivity is the issue of network performance, which refers to the efficiency of the computer network. Information technology managers are struggling with bandwidth traffic slowdowns caused by employees downloading large audio and video files from the Internet.[21] Rather than investing in greater bandwidth to increase the speed of Internet performance, some companies believe that computer monitoring and filtering technologies may be a more cost-effective solution. For example, one such company introduced a computer-monitoring product after noticing that it was taking longer to access certain Web pages and noting that its system could no longer handle sending or receiving e-mail messages containing large attachments. According to the company's IT manager, "Once we made it known that we were introducing an Internet monitoring system, employees started to think twice about accessing Web sites."[22] Clients of SurfControl, a computer monitoring technology maker, have noted different types of personal computer usage by employees,

including watching streaming video or operating Web sites from company servers, that significantly tax network resources.[23] According to the director of management studies for the AMA, "[i]t's not just a matter of corporate curiosity, but very real worries about productivity and liability that push these policies. . . Personal e-mail can clog a company's telecommunications system."[24]

iii. Workplace Liability

Potential legal liability resulting from employee computer misuse is a frequently cited concern, particularly where employees use the Internet to access inappropriate content or send such content to other employees via the corporate e-mail system. For example, brokerage Morgan Stanley was hit with a $70 million lawsuit over racist jokes that appeared on the company's e-mail system.[25] Sexual harassment claims arising from pornographic Web browsing or sexually oriented e-mails is another basis of legal liability concern. In fact, "[d]espite widespread worker education efforts that have alerted most employees to the legal pitfalls of porn in the workplace, four percent of employees in the Vault.com poll still admit to using their work computers to scan smutty sites. And 25 percent of employees said they somehow receive "improper e-mails" sometimes."[26]

Large companies have fired employees for inappropriate Internet or e-mail use including accessing inappropriate content or creating the prospect for copyright infringement liability due to the installation and use of unlicensed software. Such conduct is often detected through computer monitoring technologies.[27] For example, Dow Chemical used computer monitoring to discover that 50 employees were using the company's computers to store and send sexual or violent images. All of these employees were eventually fired.[28]

In Canada, several labour arbitration cases have focused on employee dismissal due to inappropriate computer use. In *Syndicat Canadien Des Communication de l'Energie et du Papier, section locale 552 c. CAE Electronique Lteè. (Grief du Petruzzi),*[29] a Quebec employee was dismissed from his job after his employer's routine audit of the employee's computer activities discovered that he had spent more than 50 percent of his work hours over a four month period surfing the Internet. Much of the time was spent viewing pornographic Web sites. The employer's decision to dismiss this employee was upheld by a Quebec arbitration panel.

Similarly, in *Di Vito and Mathers v. Macdonald Dettwiler & Associates*,[30] a 1996 B.C. Supreme Court case, the court upheld the dismissal of two employees for their role in circulating an e-mail containing derogatory comments about an over-weight employee. Influencing the court's decision was the fact that the employees' actions had negatively impacted their co-worker and the work environment.

iv. Confidentiality and Trade Secret Concerns

Ensuring corporate confidentiality is another oft-cited reason for using computer surveillance technologies. According to a study by the American Society for Industrial Security and PricewaterhouseCoopers, "Fortune 1000 companies sustained losses of more than $45 billion in 1999 from the theft of proprietary information – up from mid-'90s estimates from the FBI pegging the cost at roughly $24 billion a year."[31] An Intel spokesperson said, "[f]rom a policy standpoint, anything that's an Intel asset inside the

company belongs to the company. That includes the network . . .[t]he information that moves over that network is not treated as private."[32]

Concerns over the use of corporate networks to send company trade secrets or confidential data has also arisen in Canada. For example, in *Nesbitt Burns Inc. v. Lange*,[33] a 2000 Ontario Superior Court decision, Nesbitt Burns sought an interlocutory injunction to restrain a former vice-president from using its confidential information. To buttress its case for the injunction, the company used evidence that the former vice-president has misused the corporate e-mail system to solicit clients by e-mailing the clients confidential and proprietary information.

v. Computer Crime

In the wake of September 11th as well as the sharp rise in computer hacking crimes, network surveillance may also be used to help uncover crimes such as embezzlement and fraud.[34] As one author notes, "after Sept. 11, employers more than ever want to make sure that employees are not engaging in any type of criminal activity in the workplace."[35] A Canadian example of using e-mail evidence to demonstrate fraudulent employee activity occurred in *Lovelock v. DuPont Canada Inc.*, a 1998 Ontario Court of Justice (General Division) wrongful dismissal case.[36] When Lovelock challenged his firing by DuPont Canada, the company combed its e-mail records and uncovered an e-mail sent by the employee that ultimately convinced the judge of the implausibility of the employee's version of events leading to his dismissal.

vi. Legal Obligation

Under certain circumstances, employers may actually have a positive legal obligation to monitor computer usage. For example, the U.S. *Health Insurance Portability and Accountability Act* (HIPPA)[37] requires medical companies to monitor computer data in order to protect the privacy of patient information. Tags are attached to patients' data, identifying anyone that views such information. As one author suggests, "[t]hese individuals are, needless to say, monitored employees. Thus, privacy (for one group, such as patients or consumers) may be bought at the price of privacy (for another group, employees)."[38]

b. How Computer Surveillance Technologies Work

Given the widespread employer concern regarding employee computer usage, it should come as little surprise to find that companies have quickly filled the marketplace with dozens of different products that offer employers the opportunity to easily monitor their employees' computer habits.[39] The various monitoring products share several similar features. First, each can generate customizable reports that disclose how employees use their computers. For example, most products will monitor Internet activities such as how frequently employees spend time surfing the World Wide Web along with which sites they visit. Most products can also provide detailed reports about e-mail activity including the frequency of incoming and outgoing e-mail messages,[40] as well as what e-mail messages employees drafted but chose to delete prior to sending. Second, many programs also provide the employer with greater control over employees' computers by preventing them from using their computer programs in certain ways, such as by filtering out objectionable Web sites or preventing certain e-mails from being sent or received.

With a wide selection of products, companies can typically find a surveillance program to meet their particular needs. As one author notes:

> An employer primarily interested in monitoring employee productivity, for example, might prefer a very different type of surveillance device from an employer whose main concern is, say, preventing (or at least detecting) sexual harassment in the workplace. Detecting trade-secret leakage may require different technology from preventing visits to web sites that specialize in pornography or gambling.[41]

Computer surveillance programs can be broadly categorized into two groups: server-based programs that are installed on the employer's network, and client-based programs, which are installed directly on employees' computers.

i. Server-based programs

Server-based computer surveillance technologies are installed directly onto the employer's computer network. Not surprisingly, the programs focus primarily on network usage such as e-mail and Internet use. Most server-based programs restrict access to Web content based upon Internet addresses (URLs).[42] Others prevent employees from downloading specific file-types, such as movie files, graphic files, pornographic files or MP3 music files.[43]

Certain server-based programs also feature packet-sniffing software that can catch, study, and archive all communications on a network, such as e-mail, chat sessions, file sharing, and Internet browsing.[44] Since these products are placed on the company's server, employees that use their own Web-based e-mail accounts, such as Hotmail or Yahoo!, are no more secure than if they were using their company's own e-mail application program. Moreover, instant messaging discussions, using programs such as ICQ, MSN Messenger or America Online's Instant Messenger (AIM), are similarly susceptible to employer monitoring.[45]

Server-based computer monitoring technologies are particularly useful if the employer wants to simultaneously monitor the activities of a large group of users.[46] They are designed to keep logs and produce detailed reports that can identify individual employees in the event that the company's computer usage policy is breached.[47]

Some products even provide surveillance powers to employees. For example, FastTracker enables co-workers to watch each other's Internet activities with the hope that this form of peer review will deter users from straying into prohibited Web sites. FastTracker also differs from traditional server-based technologies in that it does not involve any software. Instead, a company routes all of its Internet traffic through FastTracker's site, which proceeds to log employee traffic and block access to undesirable sites.[48]

ii. Client-based programs

While server-based products are effective for detecting or preventing employees from visiting certain Web sites, they are unable to monitor activity that does not occur on the network. To monitor what programs employees are using on their personal computer without making a network connection, employers must install client-based surveillance programs directly on employees' computers that can then be used to "report back" activity to the employer.[49]

Client-based computer surveillance technologies generate logs that record all of the employees' activities to a file or database for subsequent examination. By monitoring activity regardless of whether the employee is connected to the network, the employer is able to amass far more data that encompasses a much broader range of computer uses.[50]

WinWhatWhere Investigator provides an effective illustration of how a client-based program works. The product is installed directly onto an employee's computer. As the employee uses the computer throughout the day, the program creates logs of information. In most instances, the program records the names of the software applications being used, the titles of the windows that are open on the computer, and the keystrokes that the employee enters, including those that are subsequently deleted.[51]

Some products provide graphic snapshots of what appears on the computer screen at any given time. The screenshots can then be e-mailed to the employer for investigation. Webroot WinGuardian, for example, allows the employer to review what the employee was doing at any given moment during their shift.[52] Other products allow the employer to monitor the amount of time an employee is away from the computer, or for how long the computer sits idle or is inoperative.[53] Keystroke monitoring software provides another method for employers to monitor their employees. Employers can track the number of keys each employee hits per hour on their computer, which can then be matched against company averages or expected performance levels.[54]

It is important to note that although the client-based software is installed directly onto an employee's computer, the employee may not be aware that they are being monitored. For example, Symantec's pcAnywhere allows employers to connect to personal computers along their networks without their employees' knowledge. Once connected, the employers can inspect their employees' activity in real time. Furthermore, while secretly inspecting an employee's computer use, employers can generate screen shots of the computer that can be retained for later analysis.[55] In fact, the WinWhatWhere program features a "stealth mode" that hides the program in the background. There are no toolbar tray icons or splash screens to indicate that it is working on the system. Furthermore, the product does not show up

in Windows' Close Program list or in the Add/Remove Programs window, making it even harder to detect that it is at work on the system. [56]

Part Two - Legal Approaches to Computer Surveillance in the Workplace

a. General (Mis)perceptions of Workplace Surveillance Law

Notwithstanding a relative dearth of Canadian case law on the subject, most discussion of computer and e-mail surveillance in the workplace assumes that employees enjoy little or no expectation of privacy within the workplace. As MacIsaac *et al.* note in *The Law of Privacy in Canada*:

> Many employers consider electronic mail sent and received using company computer equipment and stored on company computer networks to be the property of the employer. From the employer's perspective this is a business resource paid for by the employer and is to be used only for business purposes. Therefore, e-mail messages and telephone conversations made on behalf of the employee in the course of business should be made available for review for legitimate business and security reasons. For these reasons, an employee acting on behalf of their employer should have no reasonable expectation of privacy.[57]

This view of privacy in the workplace is not unique. In reviewing a B.C. labour arbitration involving a grievance launched by a college lab technician after being terminated for sending unwarranted allegations against other employees to a campus-wide e-mail message board, the law firm Emond Harnden summarized the case finding succinctly as "office e-mail: no reasonable expectation of privacy."[58] Although some authors, most notably Charles Morgan, have begun to suggest that employees may in fact enjoy some privacy protections in the workplace, that perspective has met with some resistance.[59]

i. Workplace Surveillance Law in the United States

The Canadian perspective on computer surveillance in the workplace is significantly influenced by U.S. jurisprudence, where courts and legislators have been far more active in addressing the issue.[60] In *Smyth v. Pillsbury Co.*, a much-

cited 1996 Pennsylvania District court case, a Pillsbury employee was fired for exchanging e-mails with his supervisor over the company's e-mail system.[61] The e-mails were deemed unprofessional and the employee was terminated. The court upheld the termination, noting that since the communication was voluntary and there was no reasonable expectation of privacy over a company e-mail system, a "company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[62] Interestingly, the court reached this determination despite evidence that the company had assured employees that e-mail communication would not be subject to interception by management.[63]

Similarly, *Bourke* v. *Nissan Motor Corp.,* a 1993 unpublished decision of the California Court of Appeal, addressed the issue of reasonable expectation of privacy in e-mail communications in the workplace by holding that employees enjoyed no such expectation.[64] Bourke was fired after an e-mail with inappropriate content was randomly identified during a computer training session. The court upheld the termination, noting that the employee had signed a computer use agreement that restricted the use of company-owned computer equipment and software to business use only and was aware that e-mail messages could be read by someone other than the intended recipient from time to time.

United States v. *Simons*, a 1998 Virginia federal court challenge to employer monitoring, also found no reasonable expectation of privacy where a systems manager traced visits to pornographic sites from the defendant's computer.[65] The court held that the search of the defendant's computer hard drive, where more than a thousand pornographic files were found, was not in violation of his constitutional fourth amendment rights. The court held that there was no reasonable expectation of privacy since the company had an Internet policy and a legitimate business interest in preventing unauthorized employee use of the Internet.

From a U.S. statutory perspective, the *Electronic Communications Privacy Act* (ECPA) is particularly relevant.[66] Section 2511 provides that it is illegal for anyone to "intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any…electronic communication."[67] The act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system,"[68] but goes on to state that it "does not include ... any wire or oral communication."[69] The ECPA, therefore, does not address e-mails stored on a personal computer since the Act is limited to transfer of data.

Although the statute would seem to prohibit interception of e-mail or other network communications, two exceptions in the Act are relevant from a workplace perspective. First, Section 2511(2)(d) contains a consent exception, which provides that it is not unlawful to intercept the contents of electronic communications when the intercepting party has obtained the consent of one of the parties to the communication.[70] Second, Section 2511(2)(a)(i) features a business use exception, that operates when an officer, employee or agent of a provider of wire or electronic wire or electronic communication services intercepts, discloses, or uses that communication in the normal course of his employment while engaged in any activity which is necessarily incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[71]

U.S. courts have interpreted the exceptions in a manner that lends support to both corporate surveillance supporters and detractors. The leading case on the scope of consent is *Watkins* v. *L.M. Berry & Co*, a 1983 11th Circuit Court of Appeals decision that dealt with telephone monitoring.[72] Watkins received a personal phone call during business hours that was monitored by her supervisor, though Watkins was unaware of the monitoring. L.M. Berry, her employer, had communicated its monitoring policy regarding personal calls to all employees. The

policy permitted such calls and employees were assured that personal calls would not be monitored except to the extent necessary to determine whether the call was personal or business in nature.

The court concluded that Watkins did not consent to a policy of general monitoring and that when the supervisor's interception went beyond what was necessary to determine the nature of the call, it exceeded Watkins' consent. The court rejected the argument that mere knowledge of a monitoring capability constituted implied consent, stating that consent "is not to be cavalierly implied."[73] The case has been cited by supporters of surveillance to suggest that clearly obtained consent will ensure that employee monitoring is lawful, while detractors of surveillance have pointed to the court's reluctance to grant statutory protection to a broadly worded consent provision.

The business use exception has also been construed in a manner that lends support to both camps. Although seemingly targeted primarily toward telecommunications systems operators, U.S. courts have held that any employer may qualify for the exception where they provide e-mail service.[74] Moreover, courts have granted employers leeway in concluding that employee surveillance meets the business interest portion of the exception.[75] However, as noted above, the *Watkins* court also held that monitoring the actual content of the communication fell outside the purview of the exception, which was found to be limited to detecting the type (personal or business) and the frequency of the communication. Although not a workplace surveillance case, a U.S. court recently addressed the admissibility of evidence obtained using a "key logger" surveillance program of the sort described in the client-side surveillance program section above. As described by the judge, *United States v. Scarfo* presented "an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity."[76] At issue was the right for U.S. law enforcement authorities to use evidence obtained from a key logger program that recorded keystrokes as the suspect entered them on his personal computer's keyboard. Law enforcement used

the program to "catch" Scarfo's passwords to otherwise inaccessible encrypted files.

Scarfo challenged the use of the evidence on ECPA grounds. The court dismissed the challenge, ruling that the key logger program was designed to only capture information when the computer was not connected to a network. The judge assessed the underlying technology and concluded that:

> Recognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the [key logger system] KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports. To do this, the F.B.I. designed the component 'so that each keystroke was evaluated individually.' As Mr. Murch explained: The default status of the keystroke component was set so that, on entry, a keystroke was normally not recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded. Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. Since Scarfo's computer possessed no other means of communicating with another computer save for the modem, the KLS did not intercept any wire communications.[77]

ii. Workplace Surveillance Law in Canada

Although Canada does not have a direct equivalent to the ECPA, the *Criminal Code* does address communication interception in a similar manner. Section 184(1) provides that "[e]very one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offense and liable to imprisonment for a term not exceeding five years."[78] Section 183 of the *Criminal Code* defines both "intercept" and "private communication". Intercept is defined as including "the listen[ing] to, record[ing] or acquir[ing] [of] a communication, or acquir[ing] the substance, meaning or purport thereof,"[79] while "private communication" is defined as "any oral communication, or any telecommunication ... made under circumstances in which it

is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it."[80]

The definition of private communication is particularly relevant since it creates a reasonable expectation of privacy requirement in order to fall within the statutory provision. No Canadian court has definitively addressed the issue of reasonable expectation to privacy although several labour arbitrations have considered the matter.[81] The issue has arisen outside the workplace context, as the 1998 *R. v. Weir* Alberta Queen's Bench decision explored the reasonable expectation of privacy of e-mail with respect to an Internet service provider.[82] The court in that case concluded that Internet users did have such an expectation, though a lesser expectation than would attach to a first class letter. The Alberta Court of Appeal upheld the decision in 2001, though the court did not address the privacy issue in its reasons.[83]

Much like the ECPA, the *Criminal Code* also features consent and business use exceptions. Section 184(2)(c) provides that the prohibition on the interception of communications does not apply to "a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it."[84] Given the similarity to the ECPA language, U.S. case law on point, such as the *Watkins* case, might have interpretative value for a Canadian court considering this provision.[85]

The business use exception in Canada is more limited in scope than the ECPA, seemingly limited only to those who are in the business of providing communications services. Section 184(2)(c) provides that the prohibition on the interception of communication does not apply to:

> a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,
(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or
(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service.[86]

The *Criminal Code*'s anti-hacker provision may also be relevant in this context. Section 342.1(1)(b) renders it an offence for a person to fraudulently or without colour of right intercept any communication to or from a computer by means of any device. Although this section would probably cover computer surveillance in the workplace, employers who act under a good faith belief that they have the right to monitor their employees (and therefore did not knowingly act without colour of right) would likely fall outside the statute.[87]

b. <u>The Move Toward a Reasonable Expectation of Privacy in the Workplace</u>

While U.S. jurisprudence may be responsible for the general perception that employees do not enjoy a reasonable expectation of privacy in the workplace, a closer examination of emerging case law, statute, and policy, particularly in Canada, suggests that a more balanced perspective is rapidly emerging. In the U.S., the Watkins case illustrates that courts are unwilling to grant employers *carte blanche* in monitoring employees within the workplace.

Moreover, recent court decisions suggest an even greater deference to privacy interests. In *Konop v. Hawaiian Airlines*, a 2001 9th Circuit Court of Appeal decision, the court addressed an employer's use of a password obtained from an employee to access a restricted Web site.[88] The court held that the employer's access was an unlawful interception, treating a Web site transmission as a communication to others. Although the decision was withdrawn for as-yet undetermined

reasons, it indicates that courts may increasingly be willing to interpret the ECPA more broadly in the interests of privacy protection.[89]

The National Labor Relations Board is even more emphatic about balancing the rights of employers to engage in workplace surveillance with the privacy interests of employees. The NLRB General Counsel's 2000 annual report features several cases involving workplace privacy issues.[90] The decisions unanimously support privacy rights in the workplace with the NLRB concluding in several cases that "an employer's complete ban on all non-business e-mail…was overbroad and facially unlawful."[91]

At the state level, several state legislatures have begun to consider enacting statutory privacy protections for employees in the workplace. For example, the California legislature passed SB 147 in 2001, a bill that would have prevented employers from reading employee communications on their company-provided e-mail address. The bill would not have prevented a company from monitoring its workers, but rather mandated that workers receive adequate notice before they log on to their computers.[92] California Governor Gray Davis ultimately vetoed the bill, arguing that "employees in today's wired economy understand that computers provided for business purposes are company property and that their use may be monitored and controlled."[93]

Canada has enjoyed greater success on the legislative front, so much so that many Canadian employees understand that workplace surveillance may occur, but they also appreciate that statutory protections limit surveillance and provide them with some privacy rights in the workplace.

The most important source of private sector privacy rights in Canada is the newly enacted *Personal Information Protection and Electronic Documents Act*

(PIPEDA),[94] which creates national private sector privacy protections. Although the law does not take full effect until January 1, 2004, the principles that underlie the statute already affect thousands of Canadian organizations.

PIPEDA replicates the workplace surveillance balancing act between employer and employee rights by addressing the dual concerns of privacy protection and reasonable collection and use of personal data. The statute's purpose clause explicitly refers to this balance, providing that:

> The purpose of this Part [Protection of Personal Information in the Private Sector] is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[95]

Although an exhaustive examination of PIPEDA is beyond the scope of this paper, several provisions merit special attention. First and foremost, the statute features an "appropriate purposes" provision that limits the collection, use, and disclosure of personal information only for purposes that a reasonable person would consider are appropriate under the circumstances."[96] This reasonableness clause creates a critical limitation on workplace surveillance since mere employee consent to surveillance is no longer sufficient to justify unlimited surveillance activities. Rather, the provision places important restrictions on surveillance by limiting such activities to purposes that a reasonable person would consider appropriate. For example, general computer workplace surveillance, conducted under the guise of fostering a harassment free workplace may be unlawful absent some clear evidence that such surveillance is responding to a known issue.

Second, PIPEDA mandates the designation of an individual who is accountable for an organization's privacy compliance.[97] The creation of a privacy officer position in every organization has important implications for workplace

surveillance. It suggests that the collection of personal workplace data must not remain under the exclusive purview of an organization's information technology personnel, but must also include input from its privacy professional. Moreover, unauthorized access to the personal information may also be similarly limited to avoid breaching statutory privacy obligations.

Third, the statute contains several provisions that must be considered when notifying employees of workplace surveillance practices. The law requires organizations to identify the purpose of the data collection,[98] to obtain consent prior to collecting data,[99] and to limit the collection of personal information to that which is necessary for the purposes identified by the organization.[100] These provisions collectively limit what employers may collect as well as establish clear obligations to properly inform employees of surveillance practices.

The statute does contain an important exception, however, that appears to grant employers' the right to conduct reasonable employee surveillance without notice under very limited circumstances. Section 7(1)(b) of the Act provides that:

> …an organization may collect personal information without the knowledge or consent of the individual only if…it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province:[101]

Although the effect of this exception has yet to be tested, the language incorporates the concept of reasonableness in two important respects. First, collection of personal information without consent may only occur where it is reasonable to assume that knowledge would compromise the accuracy of the information. Company-wide notification of surveillance policies is very common since employers use notice as a means of limiting employees' reasonable expectation of privacy. Accordingly, this provision only becomes applicable where the employer is concerned that specific notice might compromise an investigation.

While this should rarely occur in the context of most computer surveillance, it is possible to envision a scenario where the company has reason to suspect criminal activity on the part of a particular employee and wants to implement unique surveillance measures as part of the investigation without harming the investigation.

This scenario raises the second reasonableness factor. The statute provides that not only must it be reasonable to assume that consent may harm the accuracy of the information obtained, but that the collection itself must be reasonable for purposes related to investigation of a breach of contract. This factor incorporates a reasonableness requirement into the actual surveillance such that only reasonable surveillance measures can be used. As discussed below, this suggests that an invasive surveillance approach may be unlawful where an equally effective, more privacy-friendly solution is available.

Fourth, the statute requires organizations to ensure that adequate security measures are used to protect personal data[102] and creates limits on data retention, providing that "personal information shall be retained only as long as necessary for the fulfillment of the [identified] purposes."[103] These provisions restrict what employers may do after they have already collected the data, ensuring that data cannot be retained for an unlimited time while establishing a positive obligation to ensure that unauthorized personnel cannot access the data.

Although PIPEDA may provide the broadest array of privacy protections for individual Canadians, it stands as only one of several pieces of legislation that illustrate Canada's commitment to privacy rights. The *Privacy Act*,[104] which applies similar privacy rules to the collection of personal information by government institutions, fosters respect for personal privacy with a purpose clause that states that the Act is designed to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that

information."[105]

Several federal communications statutes also touch on privacy-related issues. For example, the *Radiocommunication Act*[106] provides that "except as prescribed, no person shall intercept and make use of, or intercept and divulge, any radiocommunication, except as permitted by the originator of the communication or the person intended by the originator of the communication to receive it."[107] The *Telecommunications Act*,[108] meanwhile, sets as one of its objectives that "[i]t is hereby affirmed that telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty and that the Canadian telecommunications policy has as its objectives to… contribute to the protection of the privacy of persons."[109] Commercial statutes such as the *Bank Act*,[110] which features privacy provisions that limit the collection, use, and disclosure of customer information, and the *Canada Post Act*,[111] which states that no one may open a sealed letter between the time it is sent and the time it is received unless there is a suspicion that the mail is being used to commit an infraction or consent is obtained from the author or the intended recipient, are further illustrations of privacy-oriented provisions found in federal legislation.

Canadian courts have also demonstrated their commitment to privacy protection on several occasions. In addition to the *Weir* case, in which an Alberta court ruled that e-mail enjoys a reasonable expectation of privacy, the 1999 B.C. Supreme Court decision in *Pacific Northwest Herb Corp. v. Thompson* is particularly noteworthy since the court ruled that a privacy interest in computer use may exist within the workplace.[112] The case involved a former employee of Pacific Northwest who had used a company computer in his home for both business and personal use. After the employee was fired from his position, he continued to use the computer for personal purposes, including documenting information pertaining to a wrongful dismissal action he planned to launch against his former employer. Prior to returning the computer to his former company, he retained a computer

consulting company to erase all the data contained on the computer's hard drive, including both business and personal files. Notwithstanding the attempt to erase the computer's contents, once the computer was returned to the company, his employer was able to restore the data.

The former employee sought to prevent the company from using the retrieved data, claiming both solicitor-client privilege (with respect to the wrongful dismissal documentation) and a privacy right in the materials found on the hard drive. The judge agreed, ruling that "the defendant may have a reasonable expectation of privacy in relation to those documents which were created for his own family use or personal use."[113] Interestingly, the judge reached his decision despite the fact that the employer was the acknowledged owner of the computer system.

The desire to establish a balanced approach to privacy in the workplace can also be seen in several Canadian labour arbitration decisions involving video surveillance. Although computer surveillance is better analogized to telephone surveillance given the integral role computers and e-mail now play in everyday communications, the analysis of workplace privacy rights found in many video surveillance cases provide valuable insight into the increasing importance accorded more generally to the privacy rights of employees.

One of the first labour arbitration cases to consider these issues was *Re Doman Forest Products Ltd*, a 1990 B.C. decision.[114] With privacy legislation such as PIPEDA more than a decade away, the arbitrator relied upon fundamental Charter values, particularly the affirmation of the importance of informational privacy in the 1990 *R. v. Duarte* Supreme Court of Canada decision,[115] to conclude that "electronic surveillance by the state is a breach of an individual's right to privacy and will only be countenanced by application of the standard of reasonableness."[116] Applying those principles to a private employer-employee relationship, the arbitrator concluded that while a right to privacy was not an absolute, it must be "judged

against what is 'reasonable in the circumstances' and, amongst other things, is dependent upon competing interests such as 'the relationship between the parties'."[117] To determine what is reasonable under the circumstances, the arbitrator pointed to three considerations: (i) whether it was reasonable to request a surveillance; (ii) whether the surveillance was conducted in a reasonable manner; and (iii) whether any other alternatives to surveillance available to the employer.[118]

The *Doman* decision has since been cited with approval in many cases,[119] including *St. Mary's Hospital and H.E.U.*,[120] a 1997 B.C. arbitration decision. That case involved an electrician who was conducting a routine wire inspection in a hospital when he came across a cable that was unfamiliar to him. He followed the wire to a manager's office, where he discovered a video camera above the ceiling tile in the middle of the room. When the local union became aware of the surreptitious surveillance, it was outraged at what it considered to be a substantial encroachment on the privacy rights of employees. Although the camera was subsequently removed, the union filed a grievance.

The arbitrator canvassed a wide range of Canadian decisions, many of which concluded that employees' right to privacy in the workplace is not absolute and must be judged against what is reasonable in the circumstances, before distilling the state of the law on workplace surveillance into several principles. First, the arbitrator found that surveillance can be characterized in three ways. *Benign surveillance*, which is used in employee training sessions or other similar situations, is used for the benefit of employees and thus requires little justification from employers. *Security surveillance*, which typically involves open cameras designed to protect the security of both employees and the employer, are installed with the implicit consent of the workforce and is apparent to all. Most troubling is *surreptitious surveillance*, which has the greatest effect on employee privacy. The arbitrator noted that this form of surveillance requires a strict justification from the

employer, particularly if the surveillance is not targeted to any one individual but rather is general in nature. The arbitrator continued by ruling that:

> After having determined the type, purpose, place and frequency of the hidden surveillance, the balancing of interests involves the application of specific tests. The onus is on the employer to justify the encroachment upon the employees' right to privacy by demonstrating that there is a substantial problem and that there is a strong probability that surveillance will assist in solving the problem. The employer must demonstrate not only that there is cause to initiate surveillance but that it is not in contravention of any terms of the collective agreement; it must show that it has exhausted all available alternatives and that there is nothing else that can be reasonably done in a less intrusive way; and finally, it must ensure that the surveillance is conducted in a systematic and non-discriminatory manner.[121]

This decision provides a sense of how the competing interests are balanced in Canadian labour arbitrations – surveillance is permitted, but only where a substantial problem has been identified, the surveillance is likely to solve the problem, alternative approaches have been unsuccessfully pursued, and the surveillance is implemented in a fair, even-handed manner.

Although some have questioned whether the *Doman* decision and its progeny extend beyond B.C., several decisions suggest that it does. For example, in *Re Toronto Transit Commission and A.T.U., Loc. 113 (Belsito)*,[122] a 1999 Ontario labour arbitration decision, the arbitrator concluded that "[h]aving regard to all of these cases, there is ample jurisprudential support in the arbitration cases decided in Ontario for the proposition that surveillance by an employer may, in certain circumstances, infringe upon an employee's right to privacy to an unreasonable extent."[123] Similarly, in *New Flyer Industries Ltd. and C.A.W.-Canada, Loc. 3003 (Mogg)*,[124] a 2000 Manitoba decision, the arbitrator concluded that the Doman precedent was applicable within that province.

Canada's federal Privacy Commissioner has also expressed his concern with surveillance and privacy in the workplace. These views have taken on added importance since the enactment of PIPEDA, since the Commissioner is the first arbiter of complaints filed under that Act.[125] The Commissioner's 2000-01 annual

report, released in late December 2001, provides a clear indication of how he views workplace surveillance, the privacy of e-mail, and the reasonable expectation of privacy in the workplace.[126]

The Commissioner reports on one case where he was asked to address a *Privacy Act* complaint from a Department of National Defence employee over whether his employer was entitled to use and disclose his private e-mail messages in the investigation of a harassment complaint.[127] The Commissioner began his analysis of workplace surveillance of e-mails by noting that employers often justify surveillance practices by referring to the need to protect employees from harassment in the workplace. Although the Commissioner acknowledged that such protection was necessary, he cautioned that "I don't accept that protection necessarily translates into wholesale surveillance of e-mails or computer use. We accept that there are stringent limits on an employer's right to read employees' mail, eavesdrop on their telephone calls or rifle through their desk drawers. I think we have to look closely at e-mail communications to see what principles should apply there as well."[128]

In this particular case, the DND policy on the management of electronic e-mail stated that employees should have no expectation of privacy when using the e-mail system. The Commissioner noted that he was deeply troubled by the policy, adding that:

> The law on privacy has developed around the notion of the "reasonable expectation"; one of the ways that the courts determine whether privacy has been violated has been to determine first whether a person could have reasonably expected privacy in a particular place and time. But I don't agree that it follows from this that an employee's, or anyone's, privacy can be simply eradicated by telling them not to expect any. While management has the right and the responsibility to manage, it has to operate within limits, including respect for fundamental rights. It is not for management alone to determine whether an expectation of privacy is reasonable.[129]

The Commissioner expressed similar sentiments in a speech on workplace privacy in the aftermath of the events of September 11th.[130] The Commissioner noted the growing belief that Internet communications must be monitored, citing employee productivity, protection of confidential information, security, and legal liability as the primary motivators behind installing such systems. While he recognized that some surveillance is inevitable, he argued that "[d]irected, suspicion-based inquiry is preferable to wholesale monitoring and violation of privacy. A targeted investigation based on reasonable suspicion is not only less privacy-invasive, it's more effective."[131]

Part Three – Toward Establishing a Surveillance – Privacy Reasonableness Balance

The preceding discussion suggests that there are two societal trends that appear to be on a collision course. As computing and Internet use continue to grow, the popularity of computer and e-mail surveillance systems in the workplace seems likely to develop alongside, if not outpace, that growth. While recognizing the advantages and efficiencies created by new technologies, companies are clearly concerned that productivity, security, and legal liability are potential by-products of empowering employees with computers and connections to the Internet.

Meanwhile, it appears equally true that privacy will continue to emerge as a cherished societal value that individuals will not surrender without ample justification. The view that employees forfeit all personal privacy while at work seems as outdated as the mainframe computers of yesteryear. Canadian law, as embodied in legislation, case law, labour arbitrations, and public policy, has gradually accepted the premise that surveillance in the workplace – whether by video camera, server-side computer monitoring, or client-side computer monitoring – cannot be justified by simple notice. Rather, surveillance activities must meet a test of

reasonableness that aims at a balance between the concerns of employers and the privacy interests of employees.

These developments signal an important shift in analysis. While earlier cases focused primarily on whether an employee had a reasonable expectation of privacy (with many concluding that a notice advising employees that did not have any privacy was sufficient to remove any such expectation),[132] emerging analysis focuses instead on whether the surveillance itself is reasonable.

As the collision course between computer surveillance and privacy escalates, the desirability for clear criteria to judge reasonableness intensifies. Distilling the development of both the law and technology, the author submits that there are six factors that must be considered when judging the reasonableness of computer and e-mail surveillance: (i) the target of the surveillance, (ii) its purpose, (iii) alternatives to surveillance, (iv) the surveillance technology, (v) the adequacy of notice, and (vi) the implementation of the surveillance activities.

This is not to suggest that any single factor should be viewed as determinative. In certain instances, one factor may be sufficiently important to render the remaining factors less important. For example, if an employer is faced with a legal obligation to implement surveillance technology, as in the case of certain health care providers in the United States, that legitimate purpose will likely stand above the remaining factors. Similarly, if an employer does not have a well-articulated purpose for conducting surveillance, but does so largely because he or she is able, a careful examination of the remaining factors will be necessary to ensure that the proper surveillance – privacy reasonableness balance is achieved.

a. The Six Factors

i. The Surveillance Target

The target of the surveillance refers to two distinct issues. First, consideration must be given as to whether the computer surveillance is company-

wide in scope such that it affects all employees equally, or whether only certain employees are subject to the surveillance. Assuming that it is not implemented in a discriminatory manner, narrow surveillance is the preferred approach from a privacy perspective. For example, if a law firm is concerned about employee productivity, it may be unnecessary to monitor attorneys and support staff in the same manner since attorneys are typically accountable for their time through the submission of weekly dockets. Similarly, if a technology company fears that its engineers may attempt to transfer confidential data to outside sources, it may be unnecessary to monitor employees who do not have access to that type of data, such as human resource and financial personnel.

The federal Privacy Commissioner supports targeted surveillance, arguing that such an approach is not only less privacy-invasive, but also more effective. Although PIPEDA does not specifically refer to this issue, several provisions are relevant in this context. First, the general reasonableness requirement may be useful in considering whether it is reasonable to collect personal data from someone whose activities fall outside the specified purpose of the surveillance. Second, since the collection of personal information must be limited to that which is necessary for the purposes identified by the organization, overbroad surveillance could run afoul of this important provision.

In addition to general vs. specific surveillance, the target of the surveillance factor also refers to specific types of people who may only be monitored in limited circumstances by virtue of their position. As discussed in detail in part four, the judiciary provides an excellent illustration of this, since surveillance of the judiciary not only raises privacy concerns, but fundamental judicial independence considerations that may mitigate against certain forms of surveillance.

ii. Purpose of the Surveillance

Although some organizations may install new surveillance technologies without a clear rationale in mind, case law and emerging privacy policy indicates that a well-defined purpose is essential to meet the reasonableness standard. From a legislative perspective, PIPEDA's umbrella provision, which provides that the collection, use, and disclosure of personal information must be for an appropriate purpose, presupposes that there is, in fact, a purpose to the data collection. Similarly, the *St. Mary's Hospital and H.E.U.* arbitration decision treated the identification of a purpose as a stage one consideration before moving on to the more difficult portion of the reasonableness analysis.

Part one of this report identified some of the most common reasons organizations use surveillance technologies. These included employee and network performance, workplace liability, confidentiality and trade secret concerns, computer crime, legal liability, as well as legally mandated surveillance. The use of surveillance technologies in the workplace may indeed be legitimate – it falls to the employer to articulate a clear purpose that corresponds to the target of the surveillance and the technology employed.

iii. Alternatives to Surveillance

Although surveillance technologies may represent an effective method of identifying computer or network misuse, their effect on personal privacy and potentially deleterious impact on employee morale,[133] has led many to call for the exploration of less intrusive approaches before adopting a surveillance solution. The discussion in the *St. Mary's Hospital and H.E.U.* arbitration is instructive as the arbitrator concluded that "the employer must demonstrate not only that there is cause to initiate surveillance but that it is not in contravention of any terms of the collective agreement; it must show that it has exhausted all available alternatives and that there is nothing else that can be reasonably done in a less intrusive way."[134]

Similarly, in *Brewers Retail Inc. and United Brewers' Warehousing Workers' Provincial Board (Merson)*,[135] a 1999 Ontario labour arbitration decision, the arbitrator canvassed more than a dozen surveillance decisions and noted the recurring emphasis on exploring alternatives. Although acknowledging that surveillance will not always be the alternative of last resort, he concluded that "when the activity of concern takes place at work, it may be that other alternatives are more readily available to the employer, since it is in charge of the workplace and is able to manage and direct the workplace and employees. Indeed, in given circumstances, the fact that videotaping occurs at work might render it less likely to be admissible."[136]

The need to pursue less intrusive solutions was also raised by several judges during the firestorm over computer surveillance of the judiciary in the United States in 2001. In a memorandum to all Chief Judges of U.S. courts, 9th Circuit Chief Judge Mary M. Schroeder argued that:

> [m]any judges believe that less intrusive methods of administering an Internet policy ought to be pursued before actually conducting surveillance on employee Internet activity. Most court units have only just begun to educate and inform court staff about Internet concerns, particularly bandwidth usage…[s]ome judges believe we ought to give court units the opportunity to address this in the first instance before monitoring.[137]

Those arguments were echoed in a letter from Judge Edith Jones of the 5th Circuit. Commenting on the plans to install surveillance systems throughout the U.S. judiciary, Judge Jones wrote that:

> …the Committee's report does not explain why alternate, less intrusive measures to discourage Internet or computer misuse within the judiciary are impractical. For instance,…after the monitoring program became publicized, the Executive Committee issued a communiqué regarding appropriate usage that was widely disseminated throughout the judiciary. We have been told that bandwidth usage immediately and dramatically declined in response to that communiqué. If exhortation is sufficient to discourage inappropriate use, why undertake random snooping?[138]

Surveillance technologies may certainly play a role in providing organizations with the assurance that they are limiting their legal liability within the workplace and maximizing employee productivity. In striking a reasonable surveillance – privacy balance, however,

other solutions with a more moderate impact on workplace privacy may prove just as effective and should be considered before adopting the least privacy-friendly alternative.

iv. The Surveillance Technology

With dozens of surveillance technologies available, the choice of technology must also be factored into the reasonableness analysis. In certain respects, this factor repeats the objective of the third factor of pursuing the least intrusive alternative. Once the decision to adopt surveillance technologies had been made, organizations should again consider which technology will best meet its purpose while having the most moderate impact on employee privacy interests.

The requirement to adopt the most appropriate surveillance technologies is found in the European Union's Data Protection Working Party's Opinion 8/2001 on the processing of personal data in the employment context.[139] The opinion concludes that "[a]ny monitoring must be a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers…[a]ny monitoring must be carried out in the least intrusive way possible."[140]

In choosing between surveillance technologies, organizations should be mindful of the differences between server-side and client-side surveillance. While computer crime concerns may require client-side surveillance programs, as in the *Scarfo* case, network performance concerns do not necessitate similar technologies since the concern rests with the use of the network, not the specific content accessed or created by an employee. Accordingly, network performance may be better addressed through the less intrusive server-side surveillance programs.

v. Adequacy of Notice

Given the consent exceptions found in the *Criminal Code*, a fully informed consent is needed to ensure that workplace surveillance does not breach criminal law. Moreover, the privacy protections afforded by PIPEDA also mandate that organizations obtain consent in the vast majority of cases before the collection, use and disclosure of personal information.

In order to provide meaningful consent, employees must be provided with an accurate description of surveillance practices. The Australian Office of the Privacy Commissioner has provided helpful guidance for ensuring that employees understand their employer's position.[141] The Commissioner's office recommends that the following six guidelines be incorporated into corporate policies:

1. The policy should be promulgated to staff and management to ensure that it is known and understood by staff. Ideally the policy should be linked from the screen that the user sees when they log on to the network.
2. The policy should be explicit as to what activities are permitted and forbidden.
3. The policy should clearly set out what information is logged and who in the organization has rights to access the logs and content of staff e-mail and browsing activities.
4. The policy should refer to the organization's computer security policy. Improper use of e-mail may pose a threat to system security, the privacy of staff and others and the legal liability of the organization.
5. The policy should outline, in plain English, how the organization intends to monitor or audit staff compliance with its rules relating to acceptable usage of e-mail and web browsing.
6. The policy should be reviewed on a regular basis in order to keep up with the accelerating development of the Internet and information technology. The policy should be re-issued whenever significant changes are made. This would help to reinforce the message to staff.

The Commissioner's recommendations focus on ensuring that employees are aware of and understand the corporate surveillance policy along with explicit disclosure of the intended collection, use, and disclosure of the data.

Adequate notice refers not only to the existence and prominence of the notice, but to its content as well. Decisions from the NLRB's General Counsel, who has concluded that a complete ban on all non-business e-mail is overbroad and

facially unlawful, and Canada's Privacy Commissioner, who has expressed his view that companies cannot eradicate employee privacy simply by so giving notice to employees, emphasize that organizations are not free to include unlimited surveillance rights within their policies. Rather, policies must be respectful of privacy norms and seek to achieve an appropriate balance between surveillance needs and privacy interests.

vi. Implementation of the Surveillance Technologies

The installation of the appropriate surveillance technology along with adequate employee notification does not end the reasonableness analysis. Although often overlooked, consideration must also be given to the processes and safeguards that are put into place after the surveillance begins and the data begins to accumulate. The obligation to address these concerns is found most prominently in PIPEDA, which requires the identification of a privacy-point person, who is vested with the responsibility of addressing privacy issues within the organization, as well as the need to ensure adequate security of the data and appropriate data retention policies.

Concern over who might access surveillance information was a key concern of the 9th Circuit judiciary during the controversy over judicial monitoring. Chief Judge Mary M. Schroeder, in her memo to all Chief Judges throughout the United States, noted that "[m]any judges were concerned that recording and monitoring information kept by the Administrative Office would be an inevitable part of any Senate confirmation process."[142] The likelihood of such scenario is best illustrated by the New Zealand judiciary incident, where the leak of legal though potentially embarrassing computer usage led to immediate calls for judicial resignations.

In light of the new PIPEDA obligations, it is increasingly apparent that workplace surveillance cannot be treated as a technical issue to be addressed by

the organization's information technology professionals. Rather, the organization's chief privacy officer or equivalent must play an integral role in setting policy on access, security, and retention of data.

b. Conclusions – Computer Surveillance in the Workplace

In seeking to develop an appropriate approach to workplace computer surveillance, it is worth remembering that neither the right to privacy nor the right to monitor is absolute. In an age of near ubiquitous computing and Internet communication, privacy rights form an increasingly important part of our legal fabric. Whether at work or at home, however, our right to privacy is limited by other societal goals such as effective enforcement of the *Criminal Code*.

Similarly, employers often have legitimate reasons to conduct workplace computer surveillance. As computing and Internet communication also become an increasingly important part of the workplace environment, employers will have valid reasons to turn to surveillance technologies such as ensuring that the environment remains free from harassment and unlawful conduct as well as promoting efficient uses of technology.

Canadian law seeks to balance these respective interests by assessing the reasonableness of the surveillance. In years past, an employee's reasonable expectation of privacy alone was determinative. No longer. The emergence of Charter values of privacy, national privacy legislation, international privacy norms, and labour case law all point to a shift towards greater privacy protection in the workplace.

This paper argues that navigating the competing interests of employers and employees necessitates that a series of common factors be considered when faced with a claim of improper workplace surveillance or when seeking to devise an

appropriate approach to the issue. Those factors, none of which is determinative, include (i) the target of the surveillance, (ii) its purpose, (iii) alternatives to surveillance, (iv) the surveillance technology, (v) the adequacy of notice, and (vi) the implementation of the surveillance activities.

As noted at the start of this paper, former B.C. Information and Privacy Commissioner David Flaherty notes that "[s]urveillance technology is neither inherently bad nor good, but…there is both good and bad surveillance."[143] The emerging Canadian legal approach to workplace computer surveillance incorporates that perspective by simultaneously providing the necessary flexibility to establish appropriate systems, while also respecting the premium our society places on personal privacy.

Part Four – Computer Surveillance of the Judiciary in Canada

a. Computers in the Canadian Judiciary

Computers within the Canadian judiciary date back to at least the early 1980s.[144] Not surprisingly, the focus at that time was not on the surveillance and privacy issues of today. Rather, energies were focused on demystifying computers and educating the judiciary on its potential applications.[145] In those early days, computing was seen as a tool primarily for judicial administrators, who could increase efficiencies by aggregating data. In fact, one early commentary dismissed any privacy concerns, concluding that "[m]uch of the data created by computers is aggregate data, gross statistics (totals, averages) which are not an invasion of the privacy of any one individual."[146]

While a 1986 Canadian Judicial Council (CJC) predicted that "eventually each Justice on the [Supreme] Court will have a computer",[147] it soon became clear

that computers were becoming a presence within the judiciary at a much faster rate than many had anticipated. A 1988 CJC study on the use of computers by federally appointed judges reported that 11 percent of respondents had used a computer with an additional 15 percent having access to a computer.[148] Although there was much work to be done (41 percent desired access but did not have it), the report concluded that "the message here is clear: judges are beginning to use computers."[149]

Today the computer has emerged as an indispensable tool for the vast majority of judges. In many provinces, including Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Ontario, virtually all judges have their own personal computers that are used for a wide range of activities including judgment-related work, communication, and legal research.[150] Judgment-related computer work includes entering trial notes, drafting and reviewing research memoranda, as well as crafting judgments. When several members of the bench jointly participate in drafting a single judgment, collaborative word processing capabilities as well as document comparison functionality is invaluable.

Computers also play a critical role in judicial communication since many judges use email to communicate with colleagues, clerks, and staff. While some of that communication may be relatively benign, email communication is occasionally the medium of choice for highly confidential discussions. Moreover, given that many judges regularly travel on circuit to hear cases in different parts of their province, email communication is often the primary mode of personal communication between members of the judiciary and their families.

As most practitioners and law students will attest, computerized legal research has become a mainstay of the legal research process. The judiciary makes regular use of computerized legal databases such as Quicklaw along with emerging Web-based legal services such as the Canadian Legal Information

Institute. Furthermore, legal research may encompass a broad array of non-traditional materials, with the Internet providing access to an unlimited information resource.

b. Computer Surveillance of the Judiciary in Canada

Given the integral role of computers within the modern Canadian judiciary, the concerns of the 1980s appear somewhat quaint in comparison with the issues of today. The controversies involving computer surveillance of the U.S. and New Zealand judiciaries, heightened awareness not only of the privacy implications of computer and e-mail surveillance, but also of the extent to which computers have become an essential work and communication tool within the judicial branch.

In Canada, similar concerns arose following a confidential nationwide survey of court technology security conducted by the Judges Technology Advisory Committee to the CJC in November 2001.[151] The survey was distributed to 37 chief justices/chief judges as well as an additional 35 information technology managers within the Canadian judicial system. The survey, which garnered a high response rate of 55 responses, required information technology personnel to answer 208 questions, while chief justices/chief judges were asked to complete a subset of 41 questions.[152]

Although much of the study focused on security concerns, the matter of judicial computer monitoring was also raised. The responses suggested that such monitoring is not entirely absent from the Canadian judicial scene –

> 62 percent of respondents indicated that log-in and account activity by judges or judicial staff was monitored
> 29 percent of respondents indicated that dial-in and e-mail usage by judges or judicial staff was monitored
> 33 percent of respondents indicated that Internet usage by judges or judicial staff was monitored.[153]

The data was particularly troubling in light of responses regarding the adequacy of notice and implementation of computer and e-mail monitoring. Only 50 percent of respondents indicated that they had been informed that their computer activities may be monitored, only 33 percent of users were required to sign an Appropriate Use Agreement before receiving access to the computer system,[154] and a paltry 5 percent of respondents indicated that their opening log-on screen clarified the expected use of the computing equipment by judges and judicial staff.[155] Furthermore, with only 14 percent indicating that the judges or judicial staff are involved in the monitoring activity, it became apparent that the judiciary was not involved in the implementation aspect of the monitoring activities.[156]

In view of the Technology Advisory Committee's findings, it is crucial that consideration be given to how, if at all, such monitoring policies should be instituted in the Canadian judiciary. An analysis of the reasonableness of computer and e-mail surveillance must include a review of all six factors identified in part three. Most of these factors provide guidance for reviewing existing systems and implementing new ones. Factors such as whether there is adequate notice, who has access to the data generated by the monitoring activities, what technology has been adopted, what alternatives have been pursued, and what purpose the monitoring serves cannot be assessed in the abstract. Each must be considered in light of actual facts. The reasonableness of the surveillance policy will depend, in large measure, on the outcome of that assessment.

Of particular concern within the judiciary, however, is an analysis of the first of the six factors – the surveillance target. Special consideration must be given to the appropriateness of any computer surveillance of members of the judiciary given the importance placed on judicial independence within a free and democratic society. Moreover, if it is concluded that computer surveillance of the judiciary may be reasonable in certain circumstances, that factor will directly influence the analysis of

the remaining five factors, including whether a computer surveillance policy ought to be applied in a like manner to all court personnel or whether distinctions should be made between judges, judicial clerks, and other court staff.

i. Judicial Independence

Several sources, including international treaty and Canadian law point to the importance of an independent judiciary and the potential impact of computer surveillance on that value. At the international level, the Universal Declaration on the Independence of Justice, adopted at the First World Conference on the Independence of Justice in 1983, states at Article 1.17 (b) that "[s]tates and other external authorities shall respect and protect the secrecy and confidentiality of the courts' deliberations at all stages."[157] This provision has potential applicability for computer surveillance of the judiciary where such surveillance captures data related to court deliberations, including logging of draft judgments and communications between judges on matters related to deliberations. Moreover, the reference to external authorities within the provision reinforces the need to limit access to any data generated by surveillance activities.

The Canadian Supreme Court has had the opportunity to consider the matter of judicial independence on several occasions. In *Valente v. The Queen*,[158] Justice LeDain, speaking for the court, noted that the Canadian conception of judicial independence has both an individual and institutional component. He elaborated that:

> It is generally agreed that judicial independence involves both individual and institutional relationships: the individual independence of a judge, as reflected in such matters as security of tenure, and the institutional independence of the court or tribunal over which he or she presides, as reflected in its institutional or administrative relationships to the executive and legislative branches of government.[159]

LeDain's comments were echoed by Justice McLachlin in *MacKeigan v. Hickman*,[160] which considered the importance of deliberative secrecy as part of a provincial inquiry into the wrongful conviction of Donald Marshall. Justice McLachlin summarized the state of Canadian law by reiterating the individual and institutional components of judicial independence and warning that "[a]ctions by other branches of government which undermine the independence of the judiciary therefore attack the integrity of our Constitution. As protectors of our Constitution, the Courts will not consider such intrusions lightly."[161]

Justice Cory's dissent in *MacKeigan*, which addressed the topic of the privilege of the judiciary on administrative matters, is also noteworthy since it illustrates that judicial immunity extends beyond to adjudicative judicial activities to include administrative functions such as conversations with staff, colleagues, and clerks:

> …a large measure of judicial immunity from testifying in respect of the administration of the work of the courts is an important and necessary factor in the functioning of the judicial system. For example, it would be unthinkable that an outside agency, whether it be a ministry of government, an agency of government or a bar associate, could designate which judge was to hear a particular case or which members of an appellate court were to sit on an appeal of a case. It is important that there be immunity for judges with regard to their conversations with administrative staff, as much as with their colleagues and clerks.[162]

Canadian courts have applied the Supreme Court's analysis in the context of considering the confidentiality that attaches to judges' hearing notes and other documentation. In *Canada (Privacy Commissioner) v. Canada (Labour Relations Board)*,[163] the Federal Court, Trial Division considered a request for the release of hearing notes of an adjudicator at the Canadian Labour Relations Board. Citing both *Valente* and *MacKeigan*, the court commented that:

> Judges must be in a position to take notes free from any intrusion and in particular, free from the fear that the notes could thereafter be subject to disclosure for purposes other than that for which they were intended. A judge must have total freedom as to what is and what is not noteworthy and the certainty that no one

> thereafter put in question his or her wisdom in this regard…Complete liberty to decide can only exist if the judge is entirely free from interference in fact or attempted interference by any "outsider" with the way in which the judge conducts the case or makes his or her decision.[164]

Applied to the issue of computer surveillance of the judiciary, the case law indicates that content-based monitoring, including the content of e-mails and word processed documents must invariably enjoy full confidentiality. Since computer surveillance must first capture data in order to determine whether it meets that standard, virtually all surveillance of judicial content runs the risk of breaching judicial immunity.

That is not to say that no computer monitoring of the judiciary may be feasible. While client-side programs would appear to be off-limits, it is conceivable that server-side programs that strictly monitor network usage, without regard for content, might not violate the level of confidentiality accorded to the judiciary. For such a program to be reasonable, greater analysis would be needed on the purpose of the surveillance, alternatives, adequacy of notice, and its implementation.

ii. Judicial Impartiality

Judicial independence concerns are not the only computer surveillance issue unique to the judiciary. Since judges may also be called upon to determine the legality of computer surveillance practices, there is a risk that some might question the ability of monitored judges to rule in an impartial manner. This concern is particularly pronounced where judges finds themselves ruling on the same surveillance policy to which they themselves are subject.

Interestingly, a recent Ontario Labour Relations Board (OLRB) decision had occasion to consider both judicial independence and impartiality issues. *Re Ontario (Management Board of Cabinet)*,[165] an October 2001 decision, illustrates the complexity of instituting surveillance policies that create the ability to access private notes, e-mail, and draft decisions of adjudicators. The Association of Management, Administrative and Professional Crown Employees of Ontario (AMAPCEO) alleged that the Province of Ontario's information technology policy of blocking e-mail between AMAPCEO and its members constituted an unfair labour practice. The complicating factor in the case was a motion by AMAPCEO that argued that the OLRB, the body responsible for adjudicating the allegation, was unable to do so in a fair manner. First, AMAPCEO noted that OLRB members were subject to the same policies that were the subject matter of the dispute. Second, and more importantly, AMAPCEO noted that "the Crown has the technical ability…and claims the right, to monitor and gain access to private notes, electronic mail, and draft decisions of adjudicators of the Board."[166] Consequently, AMAPCEO argued, the Board did not "have control over administrative decisions that significantly impact on its deliberations and therefore, does not enjoy sufficient institutional independence from the Crown."[167]

The Crown opposed the motion, arguing that while it had the technical ability to access notes, correspondence, and draft decisions, such monitoring would be wrong and contrary to its information technology practices.[168] The Crown pointed to a letter from its counsel that expanded upon the technical capability and official monitoring policy. That letter acknowledged that the Crown had the technical capability of monitoring computerized draft decisions, notes, as well as internal and external correspondence. It argued, however, that such monitoring was not contemplated nor authorized by ministry policies. The letter also sought to assure the Board that potential auditing of computer network usage would not include text files and would require a dual-sign off so that Board personnel would participate in the process.[169]

The Board sided with the Crown, dismissing both AMAPCEO claims, but only after engaging in some interesting discussion, particularly with respect to whether the ability to monitor impeded the Board's ability to function in a sufficiently independent manner. On the impartiality concerns raised by being subject to the same Province of Ontario Information Technology policy, the Board concluded that "decision-makers build jurisprudence that has some lasting impact on the landscape of the law. As citizens of the Province, adjudicators may some day be affected by the changes in the legal landscape in which they have participated. But that potential to be affected by a decision does not exclude judges from hearing a case."[170]

The impact of computer monitoring on institutional independence presented a thornier challenge. Although the Board concluded that the potentially monitored data was integral to deliberative secrecy, it was ultimately comforted by the Crown's stated policy of not monitoring or doing so only with safeguards that would include the participation of senior Board management. The Board was mindful, however, of *Ocean Port Hotel v. British Columbia (General Manager, Liquor Control and Licensing Branch)*,[171] a recent Supreme Court of Canada decision in which the court distinguished between the degree of independence granted to administrative tribunals and that enjoyed by the courts.

The *Ocean Port Hotel* case involved a challenge to the independence of a provincial liquor appeal board. The B.C. Court of Appeal concluded that members of the liquor board lacked the necessary guarantees of independence required of administrative decision-makers imposing penalties and set aside its decision. The Supreme Court overturned, ruling that the enabling statute clearly defined the parameters for serving on the board and that there was therefore no room to import common law doctrines of independence. Animating the SCC's decision was a

distinction between administrative boards and tribunals on the one hand, and courts on the other. Speaking for a unanimous court, Chief Justice McLachlin noted that:

> Superior courts, by virtue of their role as courts of inherent jurisdiction, are constitutionally required to possess objective guarantees of both individual and institutional independence. The same constitutional imperative applies to the provincial courts…Administrative tribunals, by contrast, lack this constitutional distinction from the executive. They are, in fact, created precisely for the purpose of implementing government policy. Implementation of that policy may require them to make quasi judicial decisions. They thus may be seen as spanning the constitutional divide between the executive and judicial branches of government. However, given their primary policy-making function, it is properly the role and responsibility of Parliament and the legislatures to determine the composition and structure required by a tribunal to discharge the responsibilities bestowed upon it. While tribunals may sometimes attract Charter requirements of independence, as a general rule they do not.[172]

In light of *Ocean Port Hotel*, the Board decision left open the possibility that a well-constructed monitoring policy might provide adequate protection for a tribunal but not for a court. Moreover, implicit in the Board's decision was the belief that absent proper safeguards, computer surveillance of an adjudicative body, whether tribunal or court, would have an adverse impact on deliberative secrecy and undermine that body's institutional independence.

iii. Judicial Confidentiality

In addition to judicial independence and impartiality considerations, confidentiality considerations, specific to the judiciary, must also be factored into the analysis. Although confidentiality of judicial deliberations and communications are hallmarks of an independent judiciary, judicial personnel are frequently granted access to information that they must legally keep strictly confidential.

For example, Canada's *Young Offenders Act*,[173] contains a series of provisions that mandate near-absolute secrecy of the identity of a person charged under the Act.[174] The Act contains specific provisions limiting disclosure of the information,[175] sets limitations on access to the information,[176] and even calls for the

destruction of the information when it is no longer required for the purpose for which it was disclosed.[177]

Similarly, the wiretap and electronic surveillance provisions found in the *Criminal Code* also establish strict secrecy requirements.[178] Most recently, the enactment of Canada's anti-terrorism legislation imposes several new confidentiality requirements on the judiciary. The legislation amends the Canada *Evidence Act*[179] by creating new restrictions on the disclosure of information in legal proceedings.[180]

Since the judiciary is frequently entrusted with highly sensitive information of this kind, these secrecy requirements may create further limitations on the legal ability to monitor judicial computer use and in the process collect such information. For example, were a systems administrator to access information subject to the *Young Offenders Act*, it would risk running afoul of the statute's access limitations. Although these confidentiality requirements do not create an absolute restriction against computer surveillance of the judiciary, they do add an additional layer of complexity to an already challenging issue.

iv. Recommendations

In view of international convention and Canadian jurisprudence, computer and e-mail surveillance of the judiciary is lawful in only the narrowest of circumstances. Any surveillance that limits deliberative secrecy would appear to be *per se* unlawful. That would likely include the use of client-side surveillance programs such as key stroke logging which is capable of capturing all data entered into a personal computer, including correspondence, draft judgments, and other protected documentation. Server-side surveillance programs are potentially lawful, subject to very stringent limitations. As illustrated by the *Re Ontario (Management Board of Cabinet)* decision, the implementation of such a surveillance program would require strict safeguards including limitations on access to the data

generated by the surveillance, a clear and effective notification system, an examination of less intrusive alternatives, and an appropriate purpose to the surveillance that does not trample over protections designed to ensure judicial independence.

In the context of emerging Canadian workplace surveillance law, the limitations on judicial surveillance are heightened further by an assessment of all six reasonableness factors. Since the "target" factor excludes most forms of computer surveillance, opportunities for reasonable surveillance is limited, with the remaining five factors assessed in light of a high threshold for reaching a determination that the surveillance was reasonable. Some of the strict limitations likely to be imposed on judicial computer surveillance include:

> Lawful surveillance of the judiciary should feature a well-defined purpose that does not have as its goal content-related monitoring for fear of encroaching on deliberative secrecy. Given the breadth of judicial computer uses, safe purposes would likely be limited to network performance issues, which may encompass external security threats to the network. Since network performance issues rely on aggregated information about general network usage patterns, it does not necessitate identification of individual computer users and nor track confidential or other sensitive information.
>
> Administrators should first seek to identify alternatives to computer surveillance. Network performance issues should first be addressed through education programs, so that judges and their staff are properly educated about the specific concerns of information technology personnel.
> In keeping with surveillance limited to network performance concerns, it appears likely that client-side surveillance systems would have an adverse impact on judicial independence considerations. Installation of server-side surveillance systems therefore emerges as the only current viable alternative.
>
> As a general rule, content-based monitoring of the judiciary should be avoided due to deliberative secrecy concerns. An exception may be appropriate, however, where there are reasonable grounds to suspect criminal wrongdoing.

Judges and judicial staff should be informed of the surveillance practices through clear, obvious, and consistent notices. This will require notification of computer usage policies when access to judicial computers is first provided, along with regular reminders during log-in sessions about the current policies and their implications for computer usage within the judicial workplace.

Judges and judicial staff must also play an integral role in the administration of the surveillance system with limited outside access to the data. The experience in New Zealand illustrates the impact that sensitive information about judicial conduct can have on public confidence in the court system.

Judges and judicial staff must be involved in the development and implementation of any surveillance program with information technology personnel that administer the program reporting directly to the court's chief justice.

---

[2] The views expressed herein are personal and do not necessarily reflect the opinions of the University of Ottawa or Goodmans LLP.

[1] Information and Privacy Commissioner for British Columbia, Investigation P98-012, Video Surveillance by Public Bodies: A Discussion, 31 March 1998.

[2] S. Shankland "Study: Web, e-mail monitoring spreads" *CNet* (8 July 2001), online: <http://news.com.com/2100-1001-269584.html > (date accessed: 20 January 2002).

[3] American Management Association, Press Release, "More Companies Watching Employees, American Management Association Annual Survey Reports" (18 April 2001), online: <http://www.amanet.org/press/amanews/ems2001.htm> (date accessed: 19 January 2002) [hereinafter AMA Press Release].

[4] *Ibid.*

[5] L. Keller, "Monitoring employees: Eyes in the workplace" *CNN.com*, 2 January 2001, online: <http://www.cnn.com/2001/CAREER/trends/01/02/surveillence/> (date accessed: 20 January 2002).

[6] N. A. Lewis, "Monitoring of Judiciary Computers is Backed," *New York Times*, 14 August 2001.

[7] M. Dolan, "Defiant Judges Bar Monitoring of Staff Net Use," *Los Angeles Times*, 9 August 2001.

[8] N. A. Lewis, "Plan for Web Monitoring in Courts Dropped," *New York Times*, 9 September 2001.

[9] V. Small, "Four Judges Logged on to Sex Sites," *New Zealand Herald,* 19 February 2002, online: <http://nzherald.co.nz/storydisplay.cfm?storyID=940048> (date accessed: 22 February 2002).

[10] *Ibid*.
[11] "Cabinet to Discuss Sex-Site Judge," *New Zealand Herald*, 18 February 2002, online: <http://www.nzherald.co.nz/storydisplay.cfm?storyID=939890> (date accessed: 22 February 2002).
[12] "District Court Judges Innocent in Visiting Sex Sites, says Minister," *New Zealand Herald,* 19 February 2002, online: <http://www.nzherald.co.nz/storydisplay.cfm?storyID=940107> (date accessed: 22 February 2002).
[13] V. Small, "Porn Inquiry Clears Judge," *New Zealand Herald*, 20 February 2002, online: <http://www.nzherald.co.nz/storydisplay.cfm?storyID=940245> (date accessed: 22 February 2002).
[14] AMA Press Release, supra, note 3.
[15] The cost of surveillance programs may actually be the least expensive software program on a computer system. For example, Surf Control, a program that tracks employee computer use, retails for $39.95. R. Konrad and S. Ames, "Web-based e-mail services offer employees little privacy" *CNet* (3 October 2000), online: <http://news.cnet.com/news/0-1007-200-2924978.html> (date accessed: 19 January 2002).
[16] E. J. Sinrod, "Electronic surveillance in the workplace" *USAToday.com* (18 October 2001), online: <http://www.usatoday.com/life/cyber/ccarch/2001/10/18/sinrod.htm> (date accessed: 19 January 2002).
[17] H. Chen, "Internet Use Survey 2000 -- Trends and Surprises in Workplace Web Use" *Vault.com* (1 September 2000), online: <http://vault.com/nr/main_article_detail.jsp?article_id=19331> (date accessed: 19 January 2002).
[18] *Ibid.*
[19] S. Chu, "Workers Waste 800 Million Hours on Web", *The Globe and Mail* (6 July 2000).
[20] *Ibid.*
[21] M. Seminerio, "Content filters don't just spy risqué surfing" *ZDNet* (29 November 1999), online: <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2398149,00.html> (date accessed: 19 January 2002).
[22] M. Street, "Filtering speeds up traffic" *IT Week* (15 October 2001), online: <http://www.surfcontrol.com/general/articles/Virginairship_IT_Week_Reprint_1001.pdf> (date accessed: 19 January 2002).
[23] H. Harreld, "And forgive us our trespasses" *Federal Computer Week* (5 February 2001), online: <http://www.fcw.com/fcw/articles/2001/0205/mgt-filter-02-05-01.asp> (date accessed: 19 January 2002).
[24] AMA Press Release, *supra* note 3.
[25] D. Hawkins, "Who's watching now? Hassled by lawsuits, firms probe workers' privacy" *USNews.com* (15 September 1997), online: <http://www.usnews.com/usnews/nycu/tech/articles/970915/15priv.htm> (date

accessed: 19 January 2002).
[26]Chen, *supra* note 17.
[27] B. Wallace and J. Fenton, "Analysis: Your PC could be watching you" *CNN.com* (15 November 2000), online: <http://www.cnn.com/2000/TECH/computing/11/15/desktop.tracker.idg/index.html> (date accessed: 19 January 2002).
[28]"Dow Chemical Fires 50 Over E-mail Abuse" *USA Today* (28 July 2000), online: <http://www.usatoday.com/life/cyber/tech/cti298.htm>. Other major companies that have fired employees for inappropriate computer use at work include; Xerox, which fired 40 employees for improper use of the Internet at work; and The New York Times, which fired 23 workers for sending potentially offensive e-mail on company computers. See W. Blitzer, "More employers taking advantage of new cyber-surveillance software" *CNN.com* (10 July 2000), online: <http://www.cnn.com/2000/US/07/10/workplace.eprivacy/> (date accessed: 19 January 2002).
[29] [2000] D.A.T.C. No. 15.
[30] 21 C.C.E.L. (2d) 137 (B.C.S.C. 1996).
[31] R. Konrad, "Leaks and geeks: International espionage goes high-tech" *CNet* (21 September 2000), online: <http://news.com.com/2100-1001-242620.html > (date accessed: 20 January 2002).
[32] R. Konrad and S. Ames, *supra*, note 15.
[33] [2000] O.J. No. 842.
[34] Wallace and Fenton, *supra* note 27.
[35] Sinrod, *supra* note 16.
[36] [1998] O.J. No. 4971.
[37] Public Law 104-191.
[38] A. Schulman, "Computer And Internet Surveillance in the Workplace: Rough Notes" online: <http://www.sonic.net/~undoc/survtech.htm> (last modified: 12 July 2001) (date accessed: 4 March 2002).
[39] *Ibid.*
[40] *Ibid.*
[41] *Ibid.*
[42] C. E. Dalton, "Special Report -- Preventing Corporate Network Abuse Gets Personal" *Network Magazine* (5 February 2001), online: <http://www.networkmagazine.com/article/NMG20010126S0003/1> (date accessed: 13 January 2002).
[43] Harreld, *supra* note 23.
[44] Electronic Privacy Information Center, "EPIC Workplace Privacy Page" online: <http://epic.org/privacy/workplace/default.html> (last updated: 8 January 2002) (date accessed: 4 March 2002)..
[45] Konrad and Ames, *supra* note 15.
[46] Schulman, *supra* note 38.
[47] A. Schulman, "Fatline & AltaVista: "Peer Pressure" Employee Monitoring?" *Privacy Foundation: Workplace Surveillance Project* (18 June 2001) online:

<http://www.privacyfoundation.org/workplace/technology/tech_show.asp?id=69&action=0> (date accessed: 19 January 2002).
[48] *Ibid.*
[49] Schulman, *supra* note 38.
[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*
[53] B. W. Gall, "Company E-mail and Internet Policies" *GigaLaw.com* (January 2000), online: <http://www.gigalaw.com/articles/gall-2000-01-p1.html> (date accessed: 19 January 2002).
[54] S. King, "Digital Workplace Privacy - Protect Yourself" *Emergit.com* (19 February 2001), online: <http://www.emergit.com/html/content_cur/profiles/02-19-2001_privacy.jsp> (date accessed: 19 January 2002).
[55] Dalton, *supra* note 42.
[56] Wallace and Fenton, *supra* note 27.
[57] B. MacIssac, R. Shields and K. Klein, *The Law of Privacy in Canada*, pp. 2-82 (Butterworths 2000).
[58] Emond Harnden, "Office E-mail: No Reasonable Expectation of Privacy", 4 *FOCUS: Employment Law* No. 3, p. 7 (April 2000), online <http://www.emond-harnden.com/apr00/camo.html>.
[59] C. Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use," 44 *McGill L.J.* 849 (1999).
[60] A. Rogers, "You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace " 5 *Journal of Technology Law and Policy* 1 (Spring 2000).
[61] 914 F.Supp. 97 (E.D. Pa. 1996).
[62] *Ibid.* at 101.
[63] *Ibid.* at 100-01.
[64] *Bourke v. Nissan Motor Corp.,* No. B068705 (Cal. Ct. App. July 26, 1993).
[65] 29 F.Supp.2d 324 (E.D. Va. 1998).
[66] Pub. L. 89-508 (1996).
[67] *Ibid.* s. 2511(1).
[68] *Ibid.* s. 2510(12).
[69] *Ibid*. s. 2510(12)(a).
[70] *Ibid*. s. 2511(2)(d).
[71] *Ibid*. s. 2511(2)(a)(i).
[72] 704 F.2d 577 (11th Cir. 1983).
[73] *Ibid*. at 581.
[74] *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996).
[75] Watkins, *supra* at 582-55.
[76] Criminal Action No. 00-404 (NHP) (D. N.J. 2001) online at <http://lawlibrary.rutgers.edu/fed/html/scarfo2.html-1.html>.
[77] *Ibid.*

[78] R.S.C. 1985, c.C-46, s. 184(1).
[79] *Ibid*. s. 183.
[80] *Ibid*.
[81] See, *infra*, part two (b).
[82] (1998), 213 A.R. 285, [1998] 8 W.W.R. 228.
[83] 50 W.C.B. (2d) 463.
[84] R.S.C. 1985, c.C-46, s. 184(2).
[85] Morgan, *supra*, note 59 at para. 79.
[86] R.S.C. 1985, c.C-46, s. 184(2)(c).
[87] Morgan, *supra*, note 59 at para. 87.
[88] 236 F. Supp. 1035 (9th Cir. 2001).
[89] McCutchen Update: Electronic Communications Monitoring in the Spotlight, online at <http://www.mccutchen.com/are/ecomm/konop_hawaiian_airlines_update.htm> (date accessed: 10 February 2001).
[90] Report of the General Counsel: September 1999 – September 2000, NLRB Office of the General Counsel, online at <http://www.lawmemo.com/emp/nlrb/gc2000.htm> (date accessed: 13 December 2001).
[91] *Ibid.*
[92] California Legislative Summary 2001, online at <http://www.dir.ca.gov/OD_pub/2001Summary.htm#sb147> (date accessed: 10 February 2002).
[93] *Ibid.*
[94] S.C. 2000, c. 5.
[95] *Ibid.* s. 3.
[96] *Ibid.* s. 5(3).
[97] *Ibid.* Schedule One, Principle 4.1.
[98] *Ibid.* Schedule One, Principle 4.2.
[99] *Ibid.* Schedule One, Principle 4.3.
[100] *Ibid.* Schedule One, Principle 4.4.
[101] *Ibid.* s. 7(1)(b).
[102] *Ibid.* Schedule One, Principle 4.7.
[103] *Ibid.* Schedule One, Principle 4.5.
[104] R.S.C. 1985, c.P-21.
[105] *Ibid.* s. 2.
[106] R.S.C. 1985, c. R-2.
[107] *Ibid.* s. 9(2).
[108] S.C. 1993, c. 38.
[109] *Ibid.* s. 7(i).
[110] S.C. 1991, c. 46.
[111] S.C. 1993, c. C-10.
[112] [1999] B.C.J. No. 2772.
[113] *Ibid.* at para. 26.
[114] 13 L.A.C. (4th) 275.

[115] [1990] 1 S.C.R. 945.
[116] *Ibid.* at 279.
[117] *Ibid.* at 280.
[118] *Ibid.* at 282.
[119] See, *e.g*., *Re Alberta Wheat Pool and G.W.U., Loc. 333 (Gould)* (1995), 48 L.A.C. (4th) 332 (Williams), *Re Pacific Press Ltd. and Vancouver Printing Pressmen, Assistants and Offset Workers' Union, Loc. 25 (Dales)* (1997), 64 L.A.C. (4th) 1 (Devine), *Re Toronto Transit Commission and A.T.U., Loc. 113 (Adams)* (1997), 61 L.A.C. (4th) 218 (Saltman), *Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and Professional Workers' Union, Loc. 304* (1994), 42 L.A.C. (4th) 151 (Brandt), and *Re Toronto Star Newspapers Ltd. and Southern Ontario Newspaper Guild, Loc. 87* (1992), 30 L.A.C. (4th) 306 (Springate).
[120] 64 L.A.C. (4th) 382.
[121] *Ibid*. at 399.
[122] 95 L.A.C. (4th) 402.
[123] *Ibid.* at 426.
[124] 85 L.A.C. (4th) 304.
[125] S.C. 2000, c. 5., s. 11(1).
[126] Federal Privacy Commissioner Annual Report 2000-2001, online at <http://www.privcom.gc.ca/information/ar/02_04_09_e.asp> (date accessed: 4 January 2002).
[127] *Ibid.* at 38-39.
[128] *Ibid.*
[129] *Ibid.*
[130] G. Radwanski, "Workplace Privacy in the Age of the Internet," University of Toronto Centre for Industrial Relations and Lancaster House Publishing 5th Annual Labour Arbitration Conference, 2 November 2001, Toronto, online <http://www.privcom.gc.ca/speech/02_05_a_01102_e.asp>.
[131] *Ibid.*
[132] See, *e.g., Smyth* v. *Pillsbury Co.*, *supra*, note 61.
[133] M. O'Donoghue, "Reasonableness in the Context of Workplace Privacy," Address to Workplace Privacy Infonex Conference, Toronto, 25 June 2001.
[134] 64 L.A.C. (4th) 382 at 399.
[135] 78 L.A.C. (4th) 394.
[136] *Ibid.* at para. 36.
[137] Chief Judge Mary M. Schroeder, "Clarification of AO Correspondence on Intrusion Detection System Shutdown," Memorandum of 11 July 2001 at page 4 (on file with author).
[138] Letter for Judge Edith Jones to the Honorable Edwin L. Nelson, Chairman CAT Committee, 18 August 2001 at page 3 (on file with author).
[139] Article 29 – EU Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, Adopted 13

September 2001, online <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf>.
[140] *Ibid.* at page 4.
[141] Guidelines on Workplace E-mail, Web Browsing and Privacy, Australian Office of the Privacy Commissioner, 30 March 2000, online <http://www.privacy.gov.au/internet/email/index.html>.
[142] Schroeder, *supra*, note 137.
[143] Flaherty, *supra*, note 1.
[144] P. S. Millar and C. Baar, *Judicial Administration in Canada* (McGill – Queen's University Press 1981).
[145] M. Felsky, *Computers and Law for Judges*, 1986 Canadian Judicial Council Superior Court Judges Seminar, 30 April 1986 at 1.
[146] Millar and Baar, *supra*, note 143 at 286.
[147] Felsky, *supra*, note 144 at 18.
[148] B. Franson, "The Use of Computers By Federally Appointed Judges, 1988," *Computer News for Judges*, No. 1, Fall 1988 at 2.
[149] *Ibid.*
[150] Informal survey by J. Jordan, March 2002 (on file with author).
[151] Court Technology Security: A Report of the Judges Technology Advisory Committee to the Canadian Judicial Council, 30 November 2001 (on file with author).
[152] Ibid. at 2.
[153] *Ibid.* at Table 2-27.
[154] *Ibid.* at Table 2-18.
[155] *Ibid.* at Table 2-27.
[156] *Ibid.*
[157] Judicial Independence: The Contemporary Debate, S. Shetreet and J. Deschenes, eds., (Martinus Nijhoff Publishers, Dodrecht, 1985) at 449.
[158] [1985] 2 S.C.R. 673.
[159] *Ibid*. at 687.
[160] [1989] 2 S.C.R. 796.
[161] Ibid. at 829.
[162] *Ibid.* at paras. 91, 94.
[163] [1996] 3 F.C. 609.
[164] *Ibid.* at para. 68 – 69.
[165] [2001] O.L.R.D. No. 3934.
[166] *Ibid.* at para. 2.
[167] *Ibid.*
[168] *Ibid.* at para. 5.
[169] *Ibid.*
[170] *Ibid.* at para. 29.
[171] [2001] S.C.J. No. 17.
[172] *Ibid*. at paras. 23 – 24.
[173] R.S.C. 1985, c. Y-1.

[174] *Ibid*. s. 38.
[175] *Ibid*. s. 38 (1.14).
[176] *Ibid*. s. 38 (1.15(b)).
[177] *Ibid*. s. 38 (1.15(c)).
[178] R.S.C. 1985, c. C-46, s. 187.
[179] R.S.C. 1985, c. C-5.
[180] Bill C-36, s. 37.