

THE CANADIAN BAR REVIEW

LA REVUE DU BARREAU  
CANADIEN

Vol.82

August 2003 Août

No. 2

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

Michael A. Geist<sup>1</sup>  
*Ottawa*

---

*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. This article examines the issue of computer and e-mail surveillance from a Canadian legal perspective, concluding that its legality is gradually shifting from an analysis of the target's reasonable expectation of privacy to an assessment of the reasonableness of the computer surveillance.*

---

<sup>1</sup> Michael A. Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa, Faculty of Law and Technology Counsel, Osler, Hoskin & Harcourt LLP. The author would like to thank the Canadian Judicial Council for sponsoring a study upon which this article is based; the Social Sciences and Humanities Research Council of Canada for its support through the Initiative on the New Economy grant program; the Canadian Judicial Council's Judges Technology Advisory Committee, particularly the Honourable Madam Justice Adelle Fruman, for their invaluable comments on earlier versions of this paper; William Karam, Candice Teitlebaum, and Teresa Martin for their research assistance; Rene Geist, and the participants at the Osgoode Hall Law School Speaker Series, the 3<sup>rd</sup> Annual Data Privacy and Security Summit, the CIAJ Dialogues of Justice Conference, the 4<sup>th</sup> International Conference on Law Via the Internet Conference, and the Yukon Bar and Bench Day for feedback on a presentation based on this paper. Any errors or omissions remain the sole responsibility of the author. The views expressed herein are personal and do not necessarily reflect the opinions of the University of Ottawa or of Osler, Hoskin & Harcourt LLP.

*L'importance de l'informatique et des communications par Internet a sensibilisé le public à la question de la surveillance informatique et des courriels. Cette préoccupation est particulièrement vive dans le milieu de travail, où des millions d'employés, qui travaillent à l'ordinateur et sont familiers avec les logiciels de traitement de texte et de courriel, ne savent peut-être pas que des logiciels de surveillance enregistrent leurs activités sur le réseau ou même chacune des touches qu'ils appuient. Cet article examine les questions de surveillance informatique et des courriels en droit canadien et conclut que la détermination de leur légalité semble effectuer un déplacement quant au point de vue de l'analyse. En effet, alors qu'il était usuel d'analyser le tout en fonction de l'attente raisonnable du respect de la vie privée, on remarque que l'évaluation est maintenant centrée sur le caractère raisonnable de la surveillance effectuée.*

---

### *Introduction*

#### *Part One – Computer Surveillance in the Workplace: The Why and How*

##### *a) Why Companies Deploy Computer Surveillance Technology*

- i) Employee Productivity*
- ii) Network Performance*
- iii) Workplace Liability*
- iv) Confidentiality and Trade Secret Concerns*
- v) Computer Crime*
- vi) Legal Obligation*

##### *b) How Computer Surveillance Technologies Work*

- i) Server-based programs*
- ii) Client-based programs*

#### *Part Two – Legal Approaches to Computer Surveillance in the Workplace*

##### *a) General (Mis)perceptions of Workplace Surveillance Law*

- i) Workplace Surveillance Law in the United States*
- ii) Workplace Surveillance Law in Canada*

##### *b) The Move Toward a Reasonable Expectation of Privacy in the Workplace*

#### *Part Three – Toward Establishing a Surveillance – Privacy Reasonableness Balance*

##### *a) The Six Factors*

- i) The Surveillance Target*
- ii) Purpose of the Surveillance*
- iii) Alternatives to Surveillance*
- iv) The Surveillance Technology*
- v) Adequacy of Notice*
- vi) Implementation of the Surveillance Technologies*

### *Conclusions*

---

“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- 0122

### Introduction

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.

Organizations 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.<sup>3</sup> 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.<sup>4</sup> 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.”<sup>5</sup> 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.<sup>6</sup>

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

---

<sup>2</sup> Information and Privacy Commissioner for British Columbia, Investigation P98-012, “Video Surveillance by Public Bodies: A Discussion”, online: <<http://www.oipcbc.org/investigations/reports/invrpt12.html>> (31 mars 1998).

<sup>3</sup> S. Shankland, “Study: Web, e-mail monitoring spreads”, online: *CNet* <<http://news.com.com/2100-1001-269584.html>> (8 July 2001)).

<sup>4</sup> American Management Association Press Release, “More Companies Watching Employees, American Management Association Annual Survey Reports”, online: American Management Association <<http://www.amanet.org/press/amanews/ems2001.htm>> [AMA Press Release].

<sup>5</sup> *Ibid.*

<sup>6</sup> L. Keller, “Monitoring employees: Eyes in the workplace” *CNN.com*, 2 January 2001, online: <<http://www.cnn.com/2001/CAREER/trends/01/02/surveillance/>> (date accessed: 20 January 2002).

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

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. Part one provides background on current computer and e-mail monitoring practices. It examines the primary rationales organizations 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.

---

<sup>7</sup> N. A. Lewis, "Monitoring of Judiciary Computers is Backed," *New York Times*, 14 August 2001.

<sup>8</sup> M. Dolan, "Defiant Judges Bar Monitoring of Staff Net Use," *Los Angeles Times*, 9 August 2001.

<sup>9</sup> N. A. Lewis, "Plan for Web Monitoring in Courts Dropped," *New York Times*, 9 September 2001.

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 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,<sup>10</sup> 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,<sup>11</sup> 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 organizations 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.<sup>12</sup> 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."<sup>13</sup> The survey further reported that

---

<sup>10</sup> AMA Press Release, *supra* note 4.

<sup>11</sup> R. Konrad and S. Ames, "Web-based e-mail services offer employees little privacy", online *CNet*: <<http://news.cnet.com/news/0-1007-200-2924978.html>> (3 October 2000). [Konrad and Ames]. (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).

<sup>12</sup> E.J. Sinrod, "Electronic surveillance in the workplace", online: *USA Today* <<http://www.usatoday.com/life/cyber/ccarch/2001/10/18/sinrod.htm>> (18 October 2003).

<sup>13</sup> H. Chen, "Internet Use Survey 2000 — Trends and Surprises in Workplace Web Use", online *Vault.com*: <[http://vault.com/nr/main\\_article\\_detail.jsp?article\\_id=19331](http://vault.com/nr/main_article_detail.jsp?article_id=19331)> (1 September 2000) [Chen].

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.<sup>14</sup>

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...”<sup>15</sup> The poll also found that “Canadians with Internet access at work spend an average of eight hours on-line a week, and of that, at least two hours” is spent on personal matters.<sup>16</sup>

## 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.<sup>17</sup> 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.”<sup>18</sup> 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.<sup>19</sup> 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

<sup>14</sup> *Ibid.*

<sup>15</sup> S. Chu, “Workers Waste 800 Million Hours on Web”, *The Globe and Mail* (6 July 2000).

<sup>16</sup> *Ibid.*

<sup>17</sup> M. Seminerio, “Content filters don’t just spy risqué surfing” *PC Week*, online: Elron Software Inc. <<http://www.elronsoftware.com/connection/story72a.html>>.

<sup>18</sup> M. Street, “Filtering speeds up traffic” *Management Week*, online: IT Week <[http://www.surfcontrol.com/general/articles/Virginairship\\_IT\\_Week\\_Reprint\\_1001.pdf](http://www.surfcontrol.com/general/articles/Virginairship_IT_Week_Reprint_1001.pdf)> (15 October 2001).

<sup>19</sup> H. Harreld, “And forgive us our trespasses”, online: *Federal Computer Week* <<http://www.fcw.com/fcw/articles/2001/0205/mgt-filter-02-05-01.asp>> (5 February 2001) [Harreld].

and liability that push these policies. . . Personal e-mail can clog a company's telecommunications system."<sup>20</sup>

### 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.<sup>21</sup> 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."<sup>22</sup>

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.<sup>23</sup> 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.<sup>24</sup>

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 Ltée. (Grief du Petruzzi)*,<sup>25</sup> a Quebec employee was

---

<sup>20</sup> AMA Press Release, *supra* note 4.

<sup>21</sup> D. Hawkins, "Who's watching now? Hassled by lawsuits, firms probe workers' privacy", online: *USNews.com* <<http://www.usnews.com/usnews/nycu/tech/articles/970915/15priv.htm>> (15 September 1997).

<sup>22</sup> Chen, *supra* note 12.

<sup>23</sup> B. Wallace and J. Fenton, "Analysis: Your PC could be watching you", online: *CNN.com* <<http://www.cnn.com/2000/TECH/computing/11/15/desktop.tracker.idg/index.html>> (15 November 2000) [Wallace and Fenton].

<sup>24</sup> "Dow Chemical Fires 50 Over E-mail Abuse" *Computerworld*, online: IDG.net <<http://www.idg.net/go.cgi?id=320556>> (28 July 2000). 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", online: *CNN.com* <<http://www.cnn.com/2000/US/07/10/workplace.eprivacy/>> (date accessed: 19 January 2002).

<sup>25</sup> [2000] D.A.T.C. No. 15.

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 Ltd.*,<sup>26</sup> 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."<sup>27</sup> 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."<sup>28</sup>

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*,<sup>29</sup> 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 11<sup>th</sup> 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.<sup>30</sup> As one author notes, "after Sept.

---

<sup>26</sup> 21 C.C.E.L. (2d) 137 (B.C.S.C. 1996).

<sup>27</sup> R. Konrad, "Leaks and geeks: International espionage goes high-tech" *CNet* (21 September 2000), online: *CNet* <<http://news.com.com/2100-1001-242620.html>> (21 September 2000).

<sup>28</sup> Konrad and Ames, *supra* note 11.

<sup>29</sup> [2000] O.J. No. 842.

<sup>30</sup> Wallace and Fenton, *supra* note 23.

11, employers more than ever want to make sure that employees are not engaging in any type of criminal activity in the workplace.”<sup>31</sup> 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.<sup>32</sup> 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 of 1996* (HIPPA)<sup>33</sup> 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).”<sup>34</sup>

#### b) *How Computer Surveillance Technologies Work*

Given the widespread employer concern regarding employee computer usage, it should come as little surprise to find that dozens of different products that offer employers the opportunity to easily monitor their employees’ computer habits have flooded the market.<sup>35</sup> 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,<sup>36</sup> 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

---

<sup>31</sup> Sinrod, *supra* note 12.

<sup>32</sup> [1998] O.J. No. 4971.

<sup>33</sup> U.S.C. 42 210 et seq..

<sup>34</sup> A. Schulman, “Computer And Internet Surveillance in the Workplace: Rough Notes” online: *SonicNet, Inc.* <<http://www.sonic.net/~undoc/survtch.htm>> (27 July 2001).

<sup>35</sup> *Ibid.*

<sup>36</sup> *Ibid.*

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, organizations 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.<sup>37</sup>

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).<sup>38</sup> Others prevent employees from downloading specific file-types, such as movie files, graphic files, pornographic files or MP3 music files.<sup>39</sup>

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.<sup>40</sup> 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.<sup>41</sup>

---

<sup>37</sup> *Ibid.*

<sup>38</sup> C. E. Dalton, "Special Report — Preventing Corporate Network Abuse Gets Personal" *Network Magazine*, online: *CMP Media* <<http://www.networkmagazine.com/article/NMG20010126S0003/1>> (5 February 2001).

<sup>39</sup> Harreld, *supra* note 18.

<sup>40</sup> Electronic Privacy Information Center, "Workplace Privacy" online: *Electronic Privacy Information Center* <<http://epic.org/privacy/workplace/default.html>> (28 October 2002)).

<sup>41</sup> Konrad and Ames, *supra* note 11.

Server-based computer monitoring technologies are particularly useful if the employer wants to simultaneously monitor the activities of a large group of users.<sup>42</sup> 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.<sup>43</sup>

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.<sup>44</sup>

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 establishing 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.<sup>45</sup>

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.<sup>46</sup>

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.<sup>47</sup>

---

<sup>42</sup> Schulman, *supra* note 34.

<sup>43</sup> A. Schulman, "Fatline & AltaVista: "Peer Pressure" Employee Monitoring?" *Privacy Foundation: Workplace Surveillance Project*, online: *Privacy Foundation* <[http://www.privacyfoundation.org/workplace/technology/tech\\_show.asp?id=69&action=0](http://www.privacyfoundation.org/workplace/technology/tech_show.asp?id=69&action=0)> (18 June 2001).

<sup>44</sup> *Ibid.*

<sup>45</sup> Schulman, *supra* note 34.

<sup>46</sup> *Ibid.*

<sup>47</sup> *Ibid.*

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.<sup>48</sup> 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.<sup>49</sup> 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.<sup>50</sup>

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.<sup>51</sup> 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.<sup>52</sup>

### *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

---

<sup>48</sup> *Ibid.*

<sup>49</sup> B.W. Gall, "Company E-mail and Internet Policies", online: *GigaLaw.com* <<http://www.gigalaw.com/articles/gall-2000-01-all.html>> (January 2000).

<sup>50</sup> "We Know What You Did Last Summer" *Wired News*, online: *Lycos Inc.* <<http://www.wired.com/news/politics/0,12,83,21847,00.html>> (25 September 1999).

<sup>51</sup> Dalton, *supra* note 38.

<sup>52</sup> Wallace and Fenton, *supra* note 23.

for legitimate business and security reasons. For these reasons, an employee acting on behalf of their employer should have no reasonable expectation of privacy.<sup>53</sup>

This view of privacy in the workplace is typical. 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.”<sup>54</sup> 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.<sup>55</sup>

### 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.<sup>56</sup> 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.<sup>57</sup> 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.”<sup>58</sup> 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.<sup>59</sup>

Similarly, *Bourke v. Nissan Motor Corp.*, a 1993 unpublished decision of the California Court of Appeal, addressed the issue of reasonable

---

<sup>53</sup> B. MacIssac, R. Shields and K. Klein, *The Law of Privacy in Canada*, (Scarborough: Carswell, 2000) pp. 2-82, 2-83.

<sup>54</sup> Emond Harnden, “Office E-mail: No Reasonable Expectation of Privacy”, 4 *FOCUS: Employment Law* No. 3, p. 7, online: Edmond Harnden LLP. <<http://www.emond-harnden.com/apr00/camo.html>> (April 2000)..

<sup>55</sup> C. Morgan, “Employer Monitoring of Employee Electronic Mail and Internet Use,” (1999) 44 McGill L.J. 849.

<sup>56</sup> A. Rogers, “You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace” (2000) 5:1 J. Tech. L & Pol’y. See also E. Bloom, M. Schachter & E.H. Steelman: “Competing Interests In The Post 9-11 Workplace: The New Line Between Privacy And Safety”, (2003) 29 *Wm. Mitchell L. Rev.* 897.

<sup>57</sup> 914 F.Supp. 97 (E.D. Pa. 1996).

<sup>58</sup> *Ibid.* at 101.

<sup>59</sup> *Ibid.* at 100-01.

expectation of privacy in e-mail communications in the workplace by holding that employees enjoyed no such expectation.<sup>60</sup> 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.<sup>61</sup> 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 of 1986* (ECPA) is particularly relevant.<sup>62</sup> 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."<sup>63</sup> 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,"<sup>64</sup> but goes on to state that it "does not include ... any wire or oral communication..."<sup>65</sup> 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.<sup>66</sup> 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

---

<sup>60</sup> *Bourke v. Nissan Motor Corp.*, No. B068705 (Cal. Ct. App. July 26, 1993).

<sup>61</sup> 29 F.Supp. 2d 324 (E.D. Va. 1998).

<sup>62</sup> 61 U.S.C. 18 2511.

<sup>63</sup> *Ibid.* 2511(1).

<sup>64</sup> *Ibid.* 2510(12).

<sup>65</sup> *Ibid.* 2510(12)(a).

<sup>66</sup> *Ibid.* 2511(2)(d).

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..."<sup>67</sup>

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 11<sup>th</sup> Circuit Court of Appeals decision that dealt with telephone monitoring.<sup>68</sup> *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."<sup>69</sup> 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.<sup>70</sup> Moreover, courts have granted employers leeway in concluding that employee surveillance meets the business interest portion of the exception.<sup>71</sup> 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

---

<sup>67</sup> *Ibid.* 2511(2)(a)(I).

<sup>68</sup> 704 F.2d 577 (11th Cir. 1983) [*Watkins*].

<sup>69</sup> *Ibid.* at 581.

<sup>70</sup> *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996).

<sup>71</sup> *Watkins*, *supra* note 68 at 582-55.

enforcement's use of new and advanced technology to vigorously investigate criminal activity."<sup>72</sup> 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.<sup>73</sup>

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."<sup>74</sup> Section 183 of the *Criminal Code* defines both "intercept" and "private communication". Intercept is defined to include "the listen[ing] to, record[ing] or acquir[ing] [of] a communication, or acquir[ing] the substance, meaning or purport thereof,"<sup>75</sup> 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

---

<sup>72</sup> 180 F.Supp. 2d 572 (D. N.J. 2001) at 574.

<sup>73</sup> *Ibid.* at 581-82.

<sup>74</sup> R.S.C. 1985, c.C-46, s. 184(1) [Criminal Code].

<sup>75</sup> *Ibid.* s. 183.

intercepted by any person other than the person intended by the originator to receive it.”<sup>76</sup>

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.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup>

Much like the ECPA, the *Criminal Code* also features consent and business use exceptions. Section 184(2)(a) 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.”<sup>80</sup> 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.<sup>81</sup>

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) 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) 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.<sup>82</sup>

---

<sup>76</sup> *Ibid.*

<sup>77</sup> See, *infra*, part two (b).

<sup>78</sup> [1998] 8 W.W.R. 228 (Alta Q.B.).

<sup>79</sup> [2001] 11 W.W.R. 85 (Alta C.A.).

<sup>80</sup> *Supra* note 74 s. 184(2).

<sup>81</sup> Morgan, *supra* note 55 at para. 79.

<sup>82</sup> *Criminal Code*, *supra* note 74, s. 184(2)©).

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.<sup>83</sup>

b) *The Move Toward a Reasonable Expectation of Privacy in the Workplace*

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 may yet emerge. In *Konop v. Hawaiian Airlines*, a 2001 9<sup>th</sup> 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.<sup>84</sup> The court initially held that the employer's access was an unlawful interception, treating a Web site transmission as a communication to others. Although the decision was later withdrawn as the court amended its reasoning by finding that an interception may only occur where information is transmitted rather than stored, the case illustrates that courts are increasingly willing to consider broad interpretations of the ECPA in the interests of privacy protection.<sup>85</sup>

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.<sup>86</sup> 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."<sup>87</sup>

<sup>83</sup> Morgan, *supra* note 55 at para. 87.

<sup>84</sup> 236 F.3rd. 1035 (9<sup>th</sup> Cir. 2001).

<sup>85</sup> 302 F.3d 868, 878 (9<sup>th</sup> Cir. 2002).

<sup>86</sup> National Labor Relations Board, Report of the General Counsel: September 1999 – September 2000, NLRB Office of the General Counsel, online: *LawMemo.com* <<http://www.lawmemo.com/emp/nlrb/gc2000.htm>> (accessed: 13 December 2001).

<sup>87</sup> *Ibid.*

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.<sup>88</sup> 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.”<sup>89</sup>

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, depending on the industrial sector, 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 *Personal Information Protection and Electronic Documents Act* (PIPEDA),<sup>90</sup> which creates national private sector privacy protections. Although the law will not apply to employment issues for provincially regulated business, the principles that underlie the statute already affect thousands of Canadian organizations that are federally regulated.

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.<sup>91</sup>

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

---

<sup>88</sup> 2001 Legislative Summary, online: *State of California, Department of Industrial Relations* <[http://www.dir.ca.gov/OD\\_pub/2001Summary.htm#sb147](http://www.dir.ca.gov/OD_pub/2001Summary.htm#sb147)> (accessed: 10 February 2002).

<sup>89</sup> *Ibid.*

<sup>90</sup> S.C. 2000, c. 5 [PIPEDA].

<sup>91</sup> *Ibid.* s. 3.

[collection], use, or [disclosure] of personal information only for purposes that a reasonable person would consider are appropriate under the circumstances.”<sup>92</sup> 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.<sup>93</sup> 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,<sup>94</sup> to obtain consent prior to collecting data,<sup>95</sup> and to limit the collection of personal information to that which is necessary for the purposes identified by the organization.<sup>96</sup> 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.<sup>97</sup>

---

<sup>92</sup> *Ibid.* s. 5(3).

<sup>93</sup> *Ibid.* Schedule One, Principle 4.1.

<sup>94</sup> *Ibid.* Schedule One, Principle 4.2.

<sup>95</sup> *Ibid.* Schedule One, Principle 4.3.

<sup>96</sup> *Ibid.* Schedule One, Principle 4.4.

<sup>97</sup> *Ibid.* s. 7(1)-7(1)(b).

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<sup>98</sup> 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."<sup>99</sup> 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*,<sup>100</sup> 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."<sup>101</sup>

---

<sup>98</sup> *Ibid.* Schedule One, Principle 4.7.

<sup>99</sup> *Ibid.* Schedule One, Principle 4.5.

<sup>100</sup> R.S.C. 1985, c.P-21.

<sup>101</sup> *Ibid.* s. 2.

Several federal communications statutes also touch on privacy-related issues. For example, the *Radiocommunication Act*<sup>102</sup> 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.”<sup>103</sup> The *Telecommunications Act*,<sup>104</sup> 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.”<sup>105</sup> Commercial statutes such as the *Bank Act*,<sup>106</sup> which features privacy provisions that limit the collection, use, and disclosure of customer information, and the *Canada Post Corporation Act*,<sup>107</sup> 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.<sup>108</sup> 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

---

<sup>102</sup> R.S.C. 1985, c. R-2.

<sup>103</sup> *Ibid.* s. 9(2).

<sup>104</sup> S.C. 1993, c. 38.

<sup>105</sup> *Ibid.* s. 7-7(I).

<sup>106</sup> S.C. 1991, c. 46.

<sup>107</sup> S.C. 1985, c. C-10.

<sup>108</sup> [1999] B.C.J. No. 2772. (Sup. Ct.).

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...”<sup>109</sup> 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 and I.W.A., Loc. 1-357*, a 1990 B.C. decision.<sup>110</sup> 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,<sup>111</sup> 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.”<sup>112</sup> 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’.”<sup>113</sup> 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.<sup>114</sup>

The *Doman* decision has since been cited with approval in many cases,<sup>115</sup> including *Re St. Mary’s Hospital and H.E.U.*,<sup>116</sup> a 1997 B.C.

---

<sup>109</sup> *Ibid.* at para. 26.

<sup>110</sup> 13 L.A.C. (4th) 275.

<sup>111</sup> [1990] 1 S.C.R. 30.

<sup>112</sup> *Doman*, *supra* note 110 at 279.

<sup>113</sup> *Ibid.* at 280.

<sup>114</sup> *Ibid.* at 282.

<sup>115</sup> See, e.g., *Re Alberta Wheat Pool and G.W.U., Loc. 333 (Gould)* (1995), 48 L.A.C. (4th) 332 per Williams, *Re Pacific Press Ltd. and Vancouver Printing Pressmen, Assistants and Offset Workers’ Union, Loc. 25 per Dales* (1997), 64 L.A.C. (4th) 1 per Devine, *Re Toronto Transit Commission and A.T.U., Loc. 113 (Adams)* (1997), 61 L.A.C. (4th) 218 per Saltman, *Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and*

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...<sup>117</sup>

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

---

*Professional Workers' Union*, (1994), 42 L.A.C. (4th) 151 per Brandt, and *Re Toronto Star Newspapers Ltd. and Southern Ontario Newspaper Guild*, Loc. 87 (1992), 30 L.A.C. (4th) 306 per Springate.

<sup>116</sup> 64 L.A.C. (4th) 382.

<sup>117</sup> *Ibid.* at 399.

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)*,<sup>118</sup> 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.”<sup>119</sup> Similarly, in *Re New Flyer Industries Ltd. and C.A.W.-Canada, Loc. 3003 (Mogg)*,<sup>120</sup> 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.<sup>121</sup> 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.<sup>122</sup>

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.<sup>123</sup> 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.”<sup>124</sup>

---

<sup>118</sup> 95 L.A.C. (4th) 402.

<sup>119</sup> *Ibid.* at 424.

<sup>120</sup> 85 L.A.C. (4th) 304.

<sup>121</sup> PIPEDA, *supra* note 90, s. 11(1).

<sup>122</sup> The Privacy Commissioner of Canada, *Annual Report 2000-2001*, (Ottawa: Minister of Public Works and Government Services Canada, 2001) online: *Privacy Commissioner of Canada* <[http://www.privcom.gc.ca/information/ar/02\\_04\\_09\\_e.asp](http://www.privcom.gc.ca/information/ar/02_04_09_e.asp)> (accessed: 4 January 2002).

<sup>123</sup> *Ibid.* at Part One - Report on The *Privacy Act*.

<sup>124</sup> *Ibid.*

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.<sup>125</sup>

The Commissioner expressed similar sentiments in a speech on workplace privacy in the aftermath of the events of September 11<sup>th</sup>.<sup>126</sup> 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.”<sup>127</sup>

The Commissioner returned to this issue in a May 2002 speech.<sup>128</sup> Lamenting the rising incidence of workplace computer surveillance, Radwanski argued that “[t]his is an infringement of privacy, no less so than searches of desks, lockers, clothing and personal effects. Monitoring and surveillance of employees’ e-mails and web browsing is collection and use of employees’ personal information.”<sup>129</sup>

Given these comments, it comes as little surprise that the Commissioner has used the same principles in addressing at least one PIPEDA complaint and in evaluating the “substantial similarity” of provincial privacy statutes. In a January 2003 finding, the Commissioner addressed a complaint over the installation of digital video recording

---

<sup>125</sup> *Ibid.*

<sup>126</sup> G. Radwanski, “Workplace Privacy in the Age of the Internet,” University of Toronto Centre for Industrial Relations and Lancaster House Publishing 5<sup>th</sup> Annual Labour Arbitration Conference, Toronto, online: *Privacy Commission of Canada* <[http://www.privcom.gc.ca/speech/02\\_05\\_a\\_011102\\_e.asp](http://www.privcom.gc.ca/speech/02_05_a_011102_e.asp)> (2 November 2001).

<sup>127</sup> *Ibid.*

<sup>128</sup> G. Radwanski, “Recent Decisions and Emerging Issues under New Privacy Legislation”, Lancaster House Annual Conference on Human Rights and Workplace Privacy, Toronto, online: *Privacy Commissioner of Canada* <[http://www.privcom.gc.ca/speech/02\\_05\\_a\\_020503\\_e.asp](http://www.privcom.gc.ca/speech/02_05_a_020503_e.asp)> (3 May 2002) [Radwanski].

<sup>129</sup> *Ibid.*

cameras that were installed at a company railway yard. The complainant objected to the cameras, arguing that they recorded personal information without consent. The company responded by noting that the equipment was used to reduce vandalism and theft, improve staff security, and limit the potential for damages. Moreover, the company altered the position of the cameras whenever it learned that its employees were inadvertently filmed.<sup>130</sup>

Despite those assurances, the Commissioner ruled that the complaint was well founded. In reaching his decision, the Commissioner employed a reasonableness analysis, determining that the company had not proven the existence of a real problem, but only the potential for one. Accordingly, the digital cameras were neither truly necessary nor particularly effective. Moreover, the Commissioner expressed concern that the existence of the cameras might cause employees to perceive that their actions were being observed and their privacy invaded.<sup>131</sup> Although this finding involves video surveillance rather than computer surveillance, the principle underlying the decision is equally applicable to both technologies – the Commissioner was of the view that intrusive security measures did not constitute reasonable surveillance given the particular circumstances.

The Commissioner's concern for workplace surveillance was also evident in his evaluation of provincial privacy statutes that must meet PIPEDA's substantial similarity test.<sup>132</sup> The Commissioner was outspoken in May 2003 in his opposition to privacy bills introduced by British Columbia<sup>133</sup> and Alberta,<sup>134</sup> highlighting insufficient workplace surveillance privacy protections, a matter that falls to the provinces for all businesses that are not federally regulated, as a prime area of concern.

### *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

---

<sup>130</sup> Privacy Commissioner of Canada, *PIPEDA Act* Case Summary #114: Employee Objects to Company's Use of Digital Surveillance Cameras, online: *Privacy Commissioner of Canada* < [http://www.privcom.gc.ca/cf-dc/2003/cf-dc\\_030123\\_e.asp](http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp) > (23 January 2003).

<sup>131</sup> *Ibid.*

<sup>132</sup> *PIPEDA*, *supra* note 89, s. 25(1).

<sup>133</sup> B.C. Freedom of International Privacy Association, letter to the Honourable Sandy Santori, B.C. Minister of Management Services, online: *Privacy Commissioner of Canada* < [http://www.privcom.gc.ca/media/le\\_030516\\_e.asp](http://www.privcom.gc.ca/media/le_030516_e.asp) > (15 May 2003).

<sup>134</sup> G. Radwanski, letter to the Honourable David Coultts, Alberta Minister of Government Services, online: *Privacy Commissioner of Canada* <[http://www.privcom.gc.ca/media/nr-c/2003/02\\_05\\_b\\_030527\\_e.asp](http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030527_e.asp)> (26 May 2003).

workplace seems likely to develop alongside, if not outpace, that growth. While recognizing the advantages and efficiencies created by new technologies, organizations 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),<sup>135</sup> emerging analysis focuses instead on whether the surveillance itself is reasonable.

As the conflict 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.<sup>136</sup>

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

---

<sup>135</sup> See, e.g., *Smyth v. Pillsbury Co.*, *supra* note 57.

<sup>136</sup> See Radwanski, *supra* note 127. (In May 2002, Canadian Privacy Commissioner George Radwanski proposed a four-part test that mirror some of these factors. Radwanski stated: “Any proposal to curtail or limit privacy must, in my view, meet four tests: it must be demonstrably necessary to meet a specific need, it must be likely to be effective in meeting that need, it must be proportional to the magnitude and importance of the problem, and there must be no less privacy-invasive way of achieving the same end.”).

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. For example, surveillance of the judiciary, already a contentious legal issue in the United States and New Zealand,<sup>137</sup> raises implications for judicial independence, impartiality, and confidentiality.

---

<sup>137</sup> Much like the computer surveillance controversy in the 9<sup>th</sup> Circuit, the New Zealand courts were rocked by a public scandal in 2002 when reports surfaced that several judges had accessed pornographic Web sites from their workplace computers. 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. Although none of the content accessed was illegal, the revelations garnered national headlines that

The Canadian Supreme Court has had the opportunity to consider the matter of judicial independence on several occasions. In *Valente v. The Queen*,<sup>138</sup> 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.<sup>139</sup>

LeDain's comments were echoed by Justice McLachlin in *MacKeigan v. Hickman*,<sup>140</sup> 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."<sup>141</sup>

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

---

were accompanied by calls for the resignations of the implicated judges. An immediate investigation revealed that all but one judge had accessed the content accidentally or for work-related purposes. See, V. Small, "Four Judges Logged on to Sex Sites," *New Zealand Herald*, (19 February 2002) online: <<http://nzherald.co.nz/storydisplay.cfm?storyID=940048>> (accessed: 22 February 2002); NZPA, "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).

<sup>138</sup> [1985] 2 S.C.R. 673.

<sup>139</sup> *Ibid.* at 687.

<sup>140</sup> [1989] 2 S.C.R. 796.

<sup>141</sup> *Ibid.* at 828, para. 61.

judges with regard to their conversations with administrative staff, as much as with their colleagues and clerks.<sup>142</sup>

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)*,<sup>143</sup> 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:

[J]udges must be able 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.<sup>144</sup>

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.

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 find 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)*,<sup>145</sup> 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.

---

<sup>142</sup> *Ibid.* at paras. 91, 94.

<sup>143</sup> [1996] 3 F.C. 609. (T.D.).

<sup>144</sup> *Ibid.* at para. 68-69.

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.”<sup>146</sup> 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...”<sup>147</sup>

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.<sup>148</sup> 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.<sup>149</sup>

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.”<sup>150</sup>

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

---

<sup>145</sup> [2001] O.L.R.D. No. 3934.

<sup>146</sup> *Ibid.* at para. 2.

<sup>147</sup> *Ibid.*

<sup>148</sup> *Ibid.* at para. 5.

<sup>149</sup> *Ibid.*

<sup>150</sup> *Ibid.* at para. 29.

doing so only with safeguards that would include the participation of senior Board management.

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*,<sup>151</sup> contains a series of provisions that mandate near-absolute secrecy of the identity of a person charged under the Act.<sup>152</sup> The Act contains specific provisions limiting disclosure of the information,<sup>153</sup> sets limitations on access to the information,<sup>154</sup> and even calls for the destruction of the information when it is no longer required for the purpose for which it was disclosed.<sup>155</sup> Similarly, the wiretap and electronic surveillance provisions found in the *Criminal Code* also establish strict secrecy requirements.<sup>156</sup> Most recently, the enactment of Canada's anti-terrorism legislation<sup>157</sup> imposes several new confidentiality requirements on the judiciary. The legislation amends the *Canada Evidence Act*<sup>158</sup> by creating new restrictions on the disclosure of information in legal proceedings.

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.

## 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

---

<sup>151</sup> R.S.C. 1985, c. Y-1.

<sup>152</sup> *Ibid.* s. 38.

<sup>153</sup> *Ibid.* s. 38 (1.14).

<sup>154</sup> *Ibid.* s. 38 (1.15(b)).

<sup>155</sup> *Ibid.* s. 38 (1.15(c)).

<sup>156</sup> *Criminal Code*, *supra* note 73, s. 187.

<sup>157</sup> S.C. 2001, c.41, s. 37.

<sup>158</sup> R.S.C. 1985, c. C-5.

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,<sup>159</sup> 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...”<sup>160</sup>

Similarly, in *Re Brewers Retail Inc. and United Brewers' Warehousing Workers' Provincial Board (Merson)*,<sup>161</sup> 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.”<sup>162</sup>

The need to pursue less intrusive solutions was also raised by several judges during the firestorm over computer surveillance of the judiciary in

---

<sup>159</sup> M. O'Donoghue, “Reasonableness in the Context of Workplace Privacy,” (Address to the Workplace Privacy Infonex Conference, Toronto, June 25, 2001) [unpublished].

<sup>160</sup> 64 L.A.C. (4th) 382 at 399.

<sup>161</sup> 78 L.A.C. (4th) 394.

<sup>162</sup> *Ibid.* at para. p. 420, 36.

the United States in 2001. In a memorandum to all Chief Judges of U.S. courts, 9<sup>th</sup> 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.<sup>163</sup>

Those arguments were echoed in a letter from Judge Edith Jones of the 5<sup>th</sup> 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?<sup>164</sup>

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.

---

<sup>163</sup> Chief Judge Mary M. Schroeder, "Clarification of AO Correspondence on Intrusion Detection System Shutdown," (Memorandum of July 11, 2001) [unpublished] at page 4 (on file with author) [Schroeder].

<sup>164</sup> Judge Edith Jones, letter to the Honorable Edwin L. Nelson, Chairman CAT Committee, (August 18, 2001) [unpublished] at page 3 (on file with author).

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.<sup>165</sup> 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."<sup>166</sup>

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.<sup>167</sup> 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.

---

<sup>165</sup> The Working Party "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: *The European Union on-line* <[http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs//2001/wp48en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs//2001/wp48en.pdf)>.

<sup>166</sup> *Ibid.* at p. 4.

<sup>167</sup> "Guidelines on Workplace E-mail, Web Browsing and Privacy", online: *The Office of the Federal Privacy Commissioner Australia* <<http://www.privacy.gov.au/internet/email/index.html>> (30 March 2000).

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 9<sup>th</sup> 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.”<sup>168</sup> 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.

### *Conclusions*

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 comments that “[s]urveillance technology is neither inherently bad nor good, but...there is both good and bad

---

<sup>168</sup> Schroeder, *supra* note 163.

surveillance.”<sup>169</sup> 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.

---

<sup>169</sup> Flaherty, *supra* note 1.