Chapter 4

EMPLOYEE PRIVACY IN THE DIGITAL AGE

I. Employees in Cyberspace: Meeting the Challenges of the Digital Age*

Allen Ponak[1]

This paper addresses several issues surrounding the use and abuse of the Internet in the workplace as well as the role of other new technologies in Canada. It is not intended to be an exhaustive review, but rather focuses on several cases that I have recently arbitrated. These cases reveal the workplace challenges of the technological revolution in which we have all been immersed.

If the cases have a common theme, it is privacy and the boundaries between our personal and work lives. While there has been debate about whether employees enjoy a legally protected "right" to privacy in the workplace, it is well settled that, at the very least, there is a legitimate employee interest in personal privacy while at work and that an employer's ability to intrude on personal privacy is restricted.[2] As a result, a balance must be struck between an employer's interest in efficient operations and an employee's interest in maintaining a separation between work and private life. The cases discussed in this paper raise issues about the intrusion by management into the personal space of employees, the limits of such intrusions, and the basis upon which the privacy balance between employee and employer should be assessed.

---

*An earlier version of this paper was prepared for the 26th Annual University of Calgary/Lancaster House Labour Arbitration and Policy Conference (2008).

[1]Adjunct Professor, Edwards School of Business, University of Saskatchewan, allenponak@shaw.ca.

[2]Brown & Beatty, Canadian Labour Arbitration (4th), §7:3625; Mitchnick & Etherington, Leading Cases in Arbitration §13.4.5.

Case of the Pornography Surfer

Following a seven-day hearing, this case eventually was settled between the parties on the basis of a letter decision I sent to the parties. As a result, no award was issued or published. The case involved a mid-level, non-managerial administrator (who I will refer to as the "grievor"), with 14 years of service, who worked for a public agency. He had his own office and a desktop computer, which was essential for his work. His performance evaluations in the previous five years had rated his work as very good to excellent. The policy of the agency with respect to computer use, of which the grievor agreed he was aware, was as follows:

> Computers assigned to employees are the property of the Agency and may be monitored. An employee is authorized to use the computers assigned to him or her for work related activities. You are granted access to computer resources on the basis of your assigned job responsibilities. You have the responsibility to use information resources in a professional, ethical and lawful manner.
>
> Occasional, limited, appropriate personal use of information resources is permitted when that use does not (1) interfere with your work performance; (2) interfere with the work performance of others; (3) have undue impact on business operations; or (4) violate any other provision of this policy.
>
> Viewing, sending, downloading, forwarding, saving, or storing material that is pornographic, sexually explicit, obscene, profane, fraudulent, discriminatory, intimidating, harassing or defamatory is prohibited.
>
> Employees who violate this policy are subject to discipline, up to and including dismissal.

It turned out that the grievor used his office computer for more than business matters. His computer had a substantial number of sexually explicit photos and video clips that might be best characterized as soft porn. As well, he had a number of personal letters stored on his computer that related to a private business that he was running. The suspicions of a new supervisor led to the discovery of this material. Whenever she visited the grievor's office he would minimize his computer screen so she could not see what he had been viewing. She also wondered if the grievor had too much time at his disposal since he would regularly volunteer to take on extra work. She did not confront him about her concerns, but instead decided to conduct an investigation. The grievor was not advised that he was being investigated.

The first part of the investigation focused on websites that the grievor may have been accessing. This was carried out by the agency's Information Technology (IT) department through a search of the agency's computer firewall log. Every time a computer in the agency visited any website, the firewall log would automatically record and retain the identity of the website, the computer from which the website was accessed, the date and time the website was accessed, and the date and time the website was exited. This firewall log search revealed that the grievor accessed many websites per day, the great majority of which were clearly unrelated to his work, and that the amount of time many of these websites were open was substantial. Included in the non-work websites were sites dedicated to sports, travel, stock markets, banking, radio stations, music, travel, sex, and nudity. Based on the results of this initial search, the grievor was suspended and his computer seized and searched. Found on the computer's hard drive were: personal letters; personal bank statements; letters relating to a private business that included his agency e-mail address and fax number in its letterhead; and video clips and photos that depicted naked or partially clothed men and women engaged in sex acts or in provocative poses.

After the computer and firewall search was completed, the grievor was terminated. The letter of termination cited as the main grounds for termination: (1) excessive personal use of his office computer and the Internet during working time; and (2) having inappropriate material on an agency computer. In its arguments, the employer defended its search of the grievor's computer use and called the termination appropriate for the reasons set out in the letter of dismissal. The union countered that the search of the grievor's computer and firewall logs was unjustified, that the employer had failed to establish that the grievor spent excessive personal time on his computer and that, while some discipline may have been warranted for the inappropriate material, discharge was excessive.

Two days after the hearing ended, I issued a three-page letter upholding discipline but ordering the grievor's reinstatement with conditions. I reserved on the amount of discipline to be imposed and also on whether the search of the grievor's computer activity was justifiable in the first place. With respect to the allegation of excessive time spent on non–work-related matters, I concluded that the evidence from the firewall logs failed to establish how much time actually was spent by the grievor on non-work websites.

For instance, one might log on to The Sports Network (TSN) website and leave that site up and running all day. The firewall log would show that TSN was opened at 9 a.m. and closed at 4:30 p.m., but that would tell us almost nothing about how much time an individual actually spent viewing the site. It might have been only a few seconds or it might have been all day. There was simply no way of calculating, based on the firewall log-in and log-out times, the amount of time the grievor was actively engaged on a particular website. Furthermore, the evidence of various IT experts who testified revealed that many websites regenerate themselves on their own without any human intervention. Logging on to one website—say, a radio station—and listening to music all day might show up on the firewall log as multiple websites. Thus, the number of websites recorded on a firewall log from any particular computer would not provide, in itself, good information about the number of websites that an individual might have deliberately accessed. In fact, the grievor's uncontradicted evidence was that he listened to music during the day through a radio station website and that, when he had office visitors, he would minimize the site and reduce the volume. Combined with the grievor's strong performance ratings and the lack of any indication that he was not carrying out his job duties in a timely fashion, I concluded that the employer had not established that the grievor was spending excessive time surfing the Web, rather than working.

The employer was on stronger grounds regarding the inappropriate material on the grievor's computer. The grievor admitted using his agency computer for private business matters. Even though the employer had failed to establish that the amount of usage was excessive, I concluded that having documents related to the grievor's own business on his office computer, along with a letterhead that contained his work and fax numbers, was not appropriate, regardless of the amount of time he engaged in such activities. The employer's policy permitting employees to use their office computers for personal matters did not extend to personal business activities, in my opinion. I found that use of the office computer for a personal business justified discipline.[3]

Also justifying discipline was pornography found on the grievor's office computer. Along with virtually every other arbitrator,

[3] *Mount Royal College and Mount Royal Support Staff Association* (1998) A.G.A.A. No. 12 (Ponak) and *Telus Communications and Telecommunications Workers Union* (2005) 143 L.A.C. 4th 299 (Sims).

I concluded that having such material on an office computer is entirely inappropriate and a serious workplace offense that exposes an employer to public sanction.[4] However, a careful reading of the authorities showed that the nature of the material and its distribution within the workplace play a role in the amount of discipline that is warranted. Put simply, pornography does not automatically justify termination. With respect to the material on the grievor's computer (which was entered into evidence through a disk and photo album), there was no evidence that any of the videos or photos contained illegal content. A lot of the material turned out to be from a Mr. Skin website, made famous in the movie *Knocked Up*, which specialized in clips and photos of nudity in feature films shown in mainstream theatres. There was no evidence that the grievor shared the contents of his computer with other employees or sent or received this material electronically. There was no evidence that co-workers saw this material or that it resulted in a poisoned work environment, although there was certainly such risk. I accepted the testimony of the grievor that the material was for his personal viewing only and had not been shared in the workplace.

In light of the grievor's clean record, relatively long service, and the inability of the employer to establish "time theft," I concluded that discharge was not appropriate. After I sent a letter to that effect, the parties settled, the grievor accepting a buyout package. Thus, I never had an opportunity to address whether the employer was justified in the first place in searching the grievor's computer activity and then seizing and searching his computer. I will say, however, that minimizing a computer a screen in the presence of a supervisor and volunteering for extra work seem to provide pretty thin grounds for an exhaustive computer search. This is especially so when the grievor was never even asked about what he was minimizing or why he seemed to have the time to take on additional tasks.

In addition to the issues surrounding the contents of the material found on the grievor's computer, one of the most instructive elements in this case is the complexity of assembling evidence of computer misuse. The evidence from the firewall logs was voluminous and included many boxes of printouts of the logs. The "raw"

---

[4] *City of London and CUPE, Local 101* (2001) 101 L.A.C. 4th 411 (Marcotte); *Petrucelli vs. Canadian National Railway* (2005) C.L.A.D. No. 113 (Betcherman); *Inco Ltd. and United Steelworkers of America, Local 6500* (2006) O.L.A.A. No. 366 (Brandt).

logs themselves would be indecipherable to most non-experts. Expert witnesses, who did not always agree with one another, were needed to explain how the strings of numbers on the firewall log related to different websites and could be traced to the grievor's computer. Without the expert evidence, the firewall logs would have been useless.

The Sanctity of Hotmail

Under what circumstances, if any, can an employer search an employee's personal (non-work) e-mail account? That was one of the questions we were asked to address in *Lethbridge College and Lethbridge College Faculty Association*.[5]

The case involved the dismissal of a college professor for sexual relationships with three students. The college had received a complaint from a student who alleged that the professor had taken unfair advantage of his position as her course instructor to start an affair shortly after the end of the semester. Based on the complaint, the college began an investigation and, as one of its first steps, it accessed the professor's college e-mail account remotely through the college's server. On the college account it found e-mails sent between the complaining student and the professor that related to the affair. It also found e-mails that seemed to suggest an affair between the professor and a second student.

At this point, the college seized the professor's college laptop. Using outside experts, it scrutinized the contents of the laptop's hard drive and was able to download e-mails from the professor's personal Hotmail account. Unbeknownst to the professor (and, I suspect, most people), e-mails sent and received on a computer may adhere to the computer's hard drive and can be accessed using data-dredging programs. The Hotmail messages contained information that suggested an affair with a third student.

Relevant portions from the college's computer use policy are set out below:

> Purpose
>
> The College has committed to purchasing microcomputer laptops for faculty, administrators and staff that require mobility. Because the laptop can and will leave the college facility, the responsibility for keeping

[5] (2007) 166 L.A.C. 4th 289 (Ponak).

the hardware in good working condition, for protecting the hardware and/or software and protecting the data stored on these laptops must now be shared between the faculty/staff member and the College.

Procedure

The following will be the responsibility of the faculty/staff member:

1. To use the laptop only for College related business.
2. To protect personal, confidential and sensitive information stored on the laptop.
3. To maintain a backup copy of all data stored on the laptop. The College will not maintain a copy of the data stored on the computer.

…

8. To return the laptop to the college when any change in employment occurs. This includes changing positions within the college.

Although the union did not challenge the admissibility of e-mails from the professor's college account, it took the position that the Hotmail messages should be inadmissible. Citing the Canadian Criminal Code and Alberta's Freedom of Information and Privacy legislation (FOIP), it argued that the grievor had a reasonable expectation of privacy when he used his Hotmail account and that such communication, even if conducted on his college laptop, should be beyond the employer's reach, unless obtained with a search warrant.

In its submissions, the employer took the position that the Hotmail account e-mails were admissible because the search of the computer was reasonable under a probable cause doctrine. The college knew that one student had already complained about the professor and was aware that the grievor used e-mail for communication, establishing a direct link between the search of the Hotmail account and the main allegations against the grievor. The search did not violate either the Criminal Code or FOIP, according to the employer, because it was perfectly legal for the college to take something it owned—the grievor's laptop computer—and look inside it. It was submitted that an employer does not need consent to look at its own machinery.

The arbitration board applied the balancing of interests tests set out in *Doman Forest Products and I.W.A. Local 1-357*[6] as a basis

[6] (1990) 13 L.A.C. 4th 275 (Vickers).

for our decision. The *Doman* tests, developed for surveillance situations, were cited by both parties as an appropriate framework of analysis:

1. Was it reasonable to conduct a search?
2. Were there alternative, less intrusive methods, to acquire the information being sought?
3. Was the search carried out in a reasonable manner?

In adopting this framework, we prefaced our analysis as follows (pages 15 and 16):

> We start from the premise that employees have some expectation of privacy in the receipt and transmission of emails from an internet provider that is not their employer's. Thus, it was reasonable for the Grievor to believe that emails on his hotmail account were beyond the reach of the College. In the Board's view, if the Grievor's hotmail was exclusively located on the Grievor's own private computer it would be inadmissible without the Grievor's consent. The Grievor, however, used the computer provided to him from the College for some of his hotmail email, changing the circumstances. The College computer was intended primarily for College work and it belongs to the College, factors which give the College some rights to access that computer. The Grievor's right to privacy for the contents of the College computer is not absolute. At the same time, recognizing that the policy against using the College computer for non-College matters has not been rigidly enforced (if enforced at all), the Employer's access to the contents of the computers it provides its employees is not unfettered either. The Employer's right to search the contents of an employee's computer must be balanced against an employee's expectation of privacy and is subject to a test of reasonableness. The criteria in *Doman* address the balancing of employer and employee interests for employer searches and surveillance of employees. These criteria have been widely adopted in arbitration and were cited by both parties. Accordingly, they are the basis for our analysis.

Based on the *Doman* framework, the board admitted the e-mails from the professor's Hotmail account. First, we found that the college had probable cause for a search based on evidence of sexual relationships with at least two students and suspicions regarding a third student, combined with the grievor's practice of communicating with these students by e-mail. Second, there did not seem to be any less intrusive means by which to investigate whether there were other students with whom the grievor had or was having sexual relationships. Interviews with specific students could reveal information about known or suspected relationships, but the board did not believe there were other realistic methods of

determining whether the grievor had relationships with additional students. Clearly, the employer could not try to interview hundreds of the grievor's former students, an exercise that would have been viewed as tantamount to a witch hunt and would have been far more intrusive of the grievor's privacy (especially in a relatively small community) than a search of his e-mails. Third, we did not find that the search of the grievor's Hotmail account violated the Criminal Code or FOIP or was otherwise carried out in an unreasonable manner. A far more detailed analysis of our reasoning and the parties' arguments is contained in the award.

Our decision in *Lethbridge College* was the first arbitration case of which I am aware that dealt head-on with the right to search personal e-mail accounts accessed through an employer-provided computer. Regardless of how one views the board's decision to admit the Hotmail, I believe that the use of the *Doman* tests demonstrated a viable framework for analysis. I am certain that more cases of this kind will arise in the future (how many readers have personal e-mail accounts that they occasionally access from their employer's computer?) and look forward to seeing how other arbitrators and tribunals address this issue.

The Right to Blog

How much trouble can an employee get herself into by writing nasty things about supervisors and co-workers in her personal blog? The answer, it turns out, is a lot of trouble.[7]

The grievor was an experienced administrative employee working for a department within the Alberta public service. She began a personal blog about running. For the uninitiated, a blog is a kind of personal online journal that the blogger posts on the Internet. It is available to anyone with Internet access unless the blogger, in setting up the blog, deliberately restricts the blog site to specific individuals (e.g., friends and family members). In this case, the blog contained no restrictions—it was available to anyone. The grievor used her own name, indicated where she was originally from in eastern Canada, and disclosed that she worked for the provincial government in Edmonton. This information would have made it relatively easy for anyone so interested to find out

[7] *Government of Alberta and Alberta Union of Provincial Employees ["R"]* (2008) 174 L.A.C. 4th 371 (Ponak); see also *Municipality of Chatham-Kent and CAW Canada, Local 127* (2007) 159 L.A.C. 4th 321 (Williamson).

the specific government department in which she worked. While some of the blog postings were apparently written and posted from the grievor's work computer, there was no allegation that she was writing her blog during time she should have been carrying out the duties of her job. Rather, she may have posted material during lunch hour or after hours. The majority of the blog postings were made from her home computer or from a public library computer.

Had the blog focused exclusively on the grievor's recreational activities as runner, it would not have been the employer's business. Regrettably, the blog was not restricted to running. It dealt with a variety of topics, many of which were of strictly personal interest, for example, favourite recipes, travel, and the family cat. However, over a three-month period, the grievor also commented about her managers and colleagues in very unflattering terms. The contents of her blog are presented in detail in the award itself. She referred to management as imbeciles, her supervisor as "Nurse Ratched," and her workplace as a lunatic asylum. She wrote about a number of her colleagues in extremely insulting, hurtful, and mean-spirited terms. She alluded to the gay lifestyle of one co-worker, ridiculed the sex life of another, and mocked the menopausal memory lapses of a third. Although she used aliases for her colleagues, not their real names, the individuals about whom she had written were easily identifiable to those in the department and perhaps others who interacted with the department in question.

Eventually her blog was discovered by some of her colleagues (they only had to Google the grievor's name) and brought to the attention of management. The reaction was universal revulsion at what she had written. To say her colleagues and supervisor were hurt and angry would be an understatement. After an investigation and disciplinary interview, the grievor was dismissed. The majority of the arbitration board, which I chaired, upheld the dismissal. Interestingly, the strongest arguments advanced by the union related to contractual violations in the investigation and treatment of the grievor. There was little dispute that the contents of the blog were inappropriate and justified discipline. In making our decision, we made the following comments about an employee's right to blog (page 51):

> While the Grievor has a right to create personal blogs and is entitled to her opinions about the people with whom she works, publicly displaying those opinions may have consequences within an employment relationship. The Board is satisfied that the Grievor, in expressing

> contempt for her managers, ridiculing her co-workers, and denigrating administrative processes, engaged in serious misconduct that irreparably severed the employment relationship, justifying discharge.

While in many ways this was a fairly straightforward disciplinary case, made unique mostly by the novel form of misconduct, there are two aspects of the case that warrant additional comment. First, one of the evidentiary issues that arose in the case was whether the arbitration board had been given a complete copy of the grievor's blog. When management first began investigating the grievor, it printed what it believed was the full blog from its inception. At the hearing, the grievor insisted that the blog was incomplete and that certain postings were missing. As well, a blog may have links to other blogs and also contain messages from other people who have logged onto the blog and left their comments. In the end, the completeness of the material provided to the board was not an issue, because we had most, if not all, the offensive postings that were germane to the discipline imposed. Our board was fortunate in that regard. The important point is that, in cases like this, it is important to have an expert download the blog and any material links and outside commentary, to ensure that a complete copy is available for all participants.

Second, the grievor told the arbitration board that she really did not expect many people to read her blog and certainly did not anticipate that anyone at work would see it, a dangerous and unrealistic assumption. Once a blog is posted, without restrictions, the creator loses control over who sees it, reads it, and sends it to others. The message is simple—if you do not want others to read it, do not post it on the Internet. Any competent recruiter will check a potential new employee to see what they have written and what was written about them. Web postings that boast about sexual fetishes, bar fights, or devil worship are unlikely to count in your favor. Nasty commentary about previous employers and co-workers, even if justified, may well cause a prospective employer to reject an otherwise suitable applicant. And, as was evident in the case with which we dealt, it may cost a current employee her job.

Hands Off!

New technology has created workplace challenges beyond cyberspace. Surveillance and recognition systems based on biometric characteristics have become increasingly available at affordable

cost. The University of Ottawa's Public Internet Policy and Public Interest Clinic provides the following definition on its website:[8]

> Biometrics, or the use of biological properties (e.g., fingerprints, retina scans, voice recognition) to identify individuals, are increasingly popular methods of identification. They are no longer confined to criminal law enforcement and the imagination of science fiction writers dreaming of hand-recognition as an automatic door opener and remote eye-scanning while entering a shopping mall. Businesses now use biometrics to regulate access to buildings and information. Governments are contemplating the inclusion of biometric identifiers in passports, driver's licenses, and possibly a future national ID card. Digital video surveillance is spreading in private and public places.
>
> However, biometric technologies incite fears of constant supervision, profiling and control, leading to a loss of individuality, privacy and freedom. Many people feel uneasy being scanned and are alarmed about having their bodily data digitally stored in large databases along with sensitive personal information. Many questions arise: Can we trust the accuracy of biometric technology? Who controls the collection of biometric data? And who has access to the databases and for what purpose?

I confronted many of these issues in *Canada Safeway Ltd. and United Food and Commercial Workers Union, Local 401*.[9] In May 2004, Safeway replaced its time clocks with a hand scan system at its warehouse and two manufacturing plants in Edmonton. On entry and exit of the plant, employees, instead of punching a time card, placed their hand, palm down, on an infrared scanner and entered a personal identification number (like a bankcard PIN). The surface of the scanner was a laminate material. The scanner would take a photograph of the top and side of the hand and fingers from which 90 measurements would be taken (length of fingers, width of hand, distance from knuckle to fingertip, etc.). Using a mathematical model called an algorithm, the 90 measurements would be converted into a 27-digit number. If the PIN on file matched, the employee's entrance or exit time would be recorded for payroll purposes. The whole operation, from the time the employee placed his or her hand on the scanner to the recording of the time, took less than five seconds.

The union filed a policy grievance, claiming the hand scan system was an unjustifiable invasion of personal privacy. The

---

[8] www.cippic.ca/biometrics.
[9] (2005) 145 L.A.C. 4th 296 (Ponak).

employer argued that because of serious problems with the previous time clock system, the hand scan system met a legitimate business need. It also argued that the impact on employee privacy was minimal. I used a proportionality or balancing-of-interests approach to assess whether the business reasons put forward by Safeway justified the privacy intrusion engendered by the hand scan system. My reasoning for adopting this framework was set out in the decision (page 15):

> Both parties agreed that employees have a right to privacy in the workplace, but that the protection of privacy rights is not absolute. A balance must be struck between the legitimate needs of employers and the privacy of employees. Numerous arbitrators, privacy tribunals, and courts have subscribed to this "balancing of rights" principle. Representative of this perspective are the comments of Arbitrator Burkett in *Trimac Transportation Services—Bulk Systems and Transportation Communications Union* (1999) 88 LAC (4th) 237 (Burkett) (page 260):
>
> > The recognition of employee privacy as a core workplace value, albeit one that is not absolute, has been recognized by arbitrators in awards dealing with searches, surveillance, medical examinations, and, more recently, drug testing. The ultimate determination in these awards rest on their individual facts. However, in all cases, the ultimate determination is arrived at on a balancing of the aforementioned competing impacts, with the onus upon the employer to establish that its business interest outweighs the employee's privacy interests.
>
> I concur with the above comments as an accurate statement of the prevailing arbitral approach.
>
> In assessing where the balance is to be struck in the current case, I accept the proportionality argument advanced by the Employer. It is an approach reflected in a recent decision of Office of the Privacy Commissioner of Canada in PIPEDA Case Summary #281 (2004) (page 2):
>
> > The Assistant Commissioner noted that the purpose of the Act is to balance the individual's right of privacy with respect to their personal information and the need of organizations to collect, use, or disclose personal information for appropriate purposes in the circumstances. In assessing this balance, the Assistant Commissioner reflected on whether the loss of privacy, from the collection and use of the voice print, was proportionate to the benefits the company would likely gain.
>
> I subscribe to the principle of proportionality. The more intrusive the impact on employee privacy, the greater the business rationale that must be demonstrated. Conversely, if the intrusion on employee privacy is insubstantial, the concomitant level of justification also is lower. For example, the taking and keeping of employee DNA samples

would require far greater justification than the taking and keeping of information on an employee's shoe size.

From a practical perspective, the onus was on the employer to make its case. It was difficult to refute that hand photographs and measurements were a form of biometric information the collection of which resulted in some intrusion on employee privacy. To meet its onus, Safeway had to establish that: (1) the introduction of the hand scan system was meeting a legitimate business need that could not be adequately met with other, less intrusive, methods; and (2) the intrusion on privacy was not excessive relative to the needs being met. In assessing the impact on privacy I was concerned with:

- the method used to collect the information;
- the type of personal information that was retained;
- the potential for the personal information to be used for purposes other than those for which it was intended;
- the method of storage and ultimate destruction of the personal information.

To meet its burden, Safeway called evidence about the deficiencies of the existing time card system, various alternatives that were considered and rejected, the characteristics of the hand scan system, and how the data were stored. The company was able to establish to my satisfaction that time cards were prone to "buddy punching," a form of time card cheating whereby co-workers clock in or clock out other workers in their absence, and various other ingenious techniques to beat the system. I was also convinced that a possible non-biometric substitute system using swipe cards contained serious drawbacks, including the expense of replacing lost cards and its susceptibility to buddy punching. Thus, Safeway was able to demonstrate a business rationale for introducing a hand scan system.

Detailed evidence on the hand scan system was provided through the testimony of two senior officials, including the chief scientist of the company that had developed the technology. Their evidence showed that the photograph taken of each person's hand did not capture fingerprints and that both the photograph and measurements were deleted from the system as soon as the verification process had been completed. The only information retained on the system was the 27-digit employee number generated from the hand measurements and the matching employee

PIN. The chief scientist testified that the 27-digit number could not be reverse engineered to create a photo or the measurements of the person's hand. More importantly, the number changed over time as the topography of an individual's hand changed.

The 27-digit number for any particular employee was likely to be different a year later (the system adjusted for these changes each time a person's hand was photographed) as the person aged, gained or lost weight, developed a callous, or suffered a hand injury. Furthermore, an individual's 27-digit number was not nearly as unique as a fingerprint or a retina scan. One percent of the population shares the same 27-digit number (i.e., in a worksite with 1,000 employees, 10 will have the same number). As a result, the 27-digit number is not useful for tracking or finding someone, since it is not sufficiently unique and changes over time. Nor was any other use suggested—nefarious or otherwise—for the 27-digit number beyond verifying, through the PIN, that a particular employee was who he or she claimed. The information provided by the two company experts, which was not contradicted by the union, led me to conclude that the biometric information captured through a hand scan constituted a relatively low intrusion on personal privacy and was far less of an intrusion than fingerprints, retina scans, and DNA.

Evidence was also provided by Safeway computer experts about the storage and destruction of the hand scan information. Employee PINs and the 27-digit number were kept on a computer system with significant firewall protection and very restricted access. No hand photographs or hand measurements—the raw data from which the 27-digit number was generated—were maintained on the system. The 27-digit number was discarded when an employee left Safeway employment.

Applying the proportionality test, I concluded that Safeway "has met its onus of justifying the use of a hand scanning system, notwithstanding that such a system involves some limited intrusion in employee privacy. Based on the evidence before me, I find that, in balancing the Employer's business needs with the privacy interests of the employee, the balance tips in favour of the Employer's business needs" (page 20). Accordingly, I denied the grievance.

My award was contrary to an earlier Ontario decision involving the same hand scan technology, *Dominion Colour Corporation and Teamsters Chemical, Energy and Allied Workers, Local 1880*,[10] in

[10](2003) Unreported (Tims).

which the arbitrator concluded that the employer had failed to establish that the business needs justified the loss of privacy. In *Dominion Colour*, the company did not call any evidence to support its reasons for introducing a hand scan system, but relied simply on arguments that the system was better than time cards. The absence of employer evidence on this point was a key factor in the decision. In a subsequent case, Arbitrator Tims again rejected the use of a hand scan system (*IKO Industries Ltd. and United Steelworkers of America, Local 580*).[11] In that decision, which was not available when I was deciding *Safeway*, the company did present evidence of a business justification, but that justification was found insufficient by the arbitrator to overcome the union's privacy concerns. In contrast, other arbitrators have allowed the introduction of a fingerprint scan system using similar technology (*Good Humour and United Food and Commercial Workers Union, Local 175*)[12] and a hand scan system (*407 ETR Concession Co. and CAW, Local 414*).[13] A very interesting aspect of *407 ETR* was the successful claim of a group of employees to be exempted from the system based on their religious objections to photographic images of their person. These contrasting decisions show that the debate about biometrics is far from over, although I believe that the balance of interests approach used in *Safeway* will become generally accepted.

Finally, it is worth mentioning that misinformation about the hand scanning system among employees was revealed in the course of the Safeway hearing. Despite efforts by management to explain the hand scan system in advance—through newsletters, for example—some employees believed that the system took their fingerprints and few employees had any idea of the kind of information being collected and stored. More detailed information, provided through small group meetings, may make a difference in how such systems are received.

Conclusion

The four cases highlighted in this paper provide a cross-section of the issues that are now arising in Internet and new technology cases. As stated at the outset, a common theme in these cases

[11] (2005) 140 L.A.C. 4th 393 (Tims).
[12] (2007) O.L.A.A. No. 406 (Murray).
[13] (2007) 158 L.A.C. 4th 289 (Albertyn).

is the balancing of employee privacy with employer operational needs. There are several analytical frameworks that have been adopted by arbitrators for assessing where the correct balance lies, but a consensus has yet to emerge on the framework or the outcomes. As the technology behind many issues becomes increasingly complex, the need for specialized expert evidence will rise. Understanding how a new technology works or the properties of a computer operating system often is critical to weighing the privacy questions that are being disputed. For this kind of understanding, expert witnesses will likely prove indispensable.

II. Privacy in the Age of Technology

Does it exist? Who has a right to it? Arbitrators from Canada and the United States explore issues related to employer monitoring of employee computer use and Internet access.

Moderator: **Jane H. Devlin,** NAA, Toronto, ON
Panelists: **Norman Brand,** NAA, San Francisco, CA
Alan A. Symonette, NAA, Philadelphia, PA
Michael Prihar, NAA, Granada Hills, CA
David R. Williamson, NAA, London, ON
Chris Sullivan, NAA, Vancouver, BC

In the fall of last year, Facebook surpassed Google as the Internet site on which the most time was spent: more than 700 billion minutes per month. Facebook has 600 million users worldwide. If it were a country, Facebook's population would rank behind those of China and India and ahead of that of the United States. It took 38 years for radio to reach 50 million consumers. It took television 13 years. It took Facebook two years.

Social networking has given us a new vocabulary. "Text" and "friend" were once thought to be nouns; now they're verbs. Twitter transmits messages of no more than 140 characters and, although it has been around for only five years, has almost 200 million users worldwide, and traffic of more than 140 million messages, or "tweets," daily.