Office of the Privacy Commissioner of Canada

Contributions Program

A Preliminary Exploration of Workplace Privacy Issues In Canada

Submitted by Vance Lockton and Richard S. Rosenberg
April 10, 2006

University of British Columbia
Department of Computer Science
201-2366 Main Mall
Vancouver, BC
V6T 1Z4

[redacted] / rosen@cs.ubc.ca

EXECUTIVE SUMMARY

Do Canadian employees lose fundamental human rights when they enter the workplace? The quick answer to this question is 'no'; however, this response deserves some consideration. Workers are frequently faced with background checks, drug and medical tests, and/or routine electronic surveillance of their actions, both in the physical and the online worlds. Companies looking to protect themselves from litigation or costly medical claims, as well as to maintain the proper corporate image, are increasingly scrutinizing employees' off-duty activities as well. At what point, though, does this monitoring invade the individual's right to privacy (as defined by the U.N.'s Declaration of Human Rights)? To what extent are Canadians willing to allow corporate interests to supercede those of the individual? Also, should they choose to oppose surveillance, what legal protections do Canadian employees have? The following report addresses these questions by exploring the right to privacy, including the rationale for and against workplace monitoring, noting the situations in which employee and employer interests come in to conflict, examining the relevant legislation in Canada and abroad as well as discussing instances in which court decisions have either strengthened or weakened employee rights. The report concludes by identifying some of the problems that must be solved before Canadian employees will see any true privacy protections.

Canadian workplace privacy legislation is weak, at best. As in the United States, a person's right to privacy is not protected by the Canadian Charter; rather, it is derived from a series of other rights. There are two main Acts that have been adopted in order to clarify this situation, and define the ways in which privacy is legally protected: the *Privacy Act* of 1983, and the *Personal Information Protection and Electronic Documents Act (*PIPEDA), which came into effect in part in 2001, and in full in 2004. These acts limit the collection of personal information about individuals to that which would be considered appropriate by a 'reasonable person', as well as ensuring that such collection is done after the individuals' consent has been obtained. However, these laws do not cover information collected by employers about non-federally regulated private sector employees. In fact, with the exception of workers in B.C., Alberta and Quebec, each of which has passed its own privacy legislation, Canadian private sector employees have little to no protections for their privacy rights.

This fact affects more than just the employee who is attempting to avoid completing his or her tasks. This report describes the ways in which comprehensive workplace monitoring leads to increases in employee stress and depression, decreased productivity, and a general sense of employees as machines, rather than humans. Pre-employment screening, random drug tests, regular medical examinations, continuous electronic monitoring and periodic off-duty surveillance all lead to a state in which the employee becomes dehumanized, as he or she is constantly monitored for defects and marked for corrective measures.

Employers, however, argue that this level of scrutiny is necessary and justified, as they have an equal right to protect their assets, as well as measuring workplace activity in order to ensure that employees earn their salaries. Companies also note that in order to

protect themselves from liability, they must prove that every effort has been made to create a workplace free from violence and harassment, which is best achieved through programs of surveillance.

The seeming conflict between employee and employer rights arises in many situations, and is often challenged either in court or before Canada's Privacy Commissioner. The use of closed-circuit television (CCTV), or surveillance cameras, is workplace situation that is most frequently seen by the Commissioner. The many cases that have been presented serve to form a clear set of regulations for CCTV's installation: employees must be informed of the purpose of the cameras (and that purpose must be considered 'reasonable'), the cameras cannot monitor an individual's work area, and they also cannot be used for anything but their original purpose (with exceptions for the investigation of a crime). This seems a fair situation for both employee and employer; it is hoped that it will become a model for other, less defined situations, such as mail opening, keystroke monitoring, off-duty surveillance and drug testing, all of which are discussed in the report. The report also describes the privacy protections (or complete lack thereof) for workplace e-mail communications in the United States, as a warning to Canadian lawmakers of what may be considered 'reasonable surveillance.'

Once the legal situation regarding Canadian workplace privacy has been established, the report suggests five fundamental problems that must be addressed in order to resolve the issues discovered. They are:

- The adversarial relationship between the employee and employer;
- The use of the 'reasonable person' criteria in PIPEDA;
- The Privacy Commissioner's prohibition from publishing the names of companies whose practices are challenged;
- The lack of anticipation of the privacy effects of new technologies, and;
- A lack of study of privacy in the Canadian workplace.

Though solving these problems will not be sufficient to resolve the workplace privacy crisis, such solutions will be necessary conditions for a positive outcome. Strong workplace privacy protection can be beneficial for all parties. This report is an initial attempt at providing a framework for such an effect.

TABLE OF CONTENTS

1. INTRODUCTION

> *"Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot do anything about it. Our civilization is decadent and our language – so the argument runs – must inevitably share in the general collapse. It follows that any struggle against the abuse of language is a sentimental archaism, like preferring candles to electric light or hansom cabs to aeroplanes. Underneath this lies the half-conscious belief that language is a natural growth and not an instrument which we shape for our own purposes."*
>
> - George Orwell

The introduction to George Orwell's 1946 essay 'Politics and the English Language' given above is the beginning of a call for the return of clarity and freshness to the written word. This will not be found, Orwell argues, through a maniacal compliance to and acceptance of traditional rules – rather, it will come to be when authors remove from their writing any stale, commonplace images and unnecessary complications. When authors spend time in choosing the best phrase, particularly at times when precedent dictates some other, more out-of-date course, language may once again thrive.

Modern day privacy, and particularly privacy in the workplace, is in a similar condition. It is too widely assumed that its abuse is inevitable, or that any struggle to protect it is nothing more than outdated sentimentality. Regulations are not adequately changing to reflect modern technologies, and legal precedents are being created based on outmoded analyses. The situation calls for a fresh approach, based not just on modifying existing laws, but on an examination of the changing nature of both privacy and the workplace, the rights of both the employee (to privacy) and the employer (to carry out surveillance), and the ways in which the approaches taken to this issue by Canada and others can (and should) change to create an equitable situation for both parties.

1.1. Definition of Privacy

One of the first things that must be noted when studying privacy in the workplace is that a person's 'right to privacy' is a nebulous concept, without clear definition or, often, basis in constitutional law. The well-known 1890 Warren and Brandeis definition of privacy as the 'right to be let alone' is a starting point, but we must also consider others: *Privacy Journal* editor Robert Ellis Smith calls privacy "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves" [Smith, 2000]; author Simson Garfinkle says it is the "right of people to control what details about their lives stay inside their own houses and what leaks to the outside." [Garfinkle, 2000] Dictionary definitions of privacy (e.g. "freedom from observation, intrusion, or attention of others") are particularly unhelpful in this case, as the phrase 'workplace privacy' would then become an oxymoron (as an employer certainly has the right to at least occasional observation of his or her employees). Thus, due to the fact that there is (and for all intents cannot be) a single, comprehensive definition of the meaning of the term 'privacy', it is left to judges to determine limits on what is and is not a 'violation' thereof.

Adding to the definitional confusion is the fact that in both Canada and the United States, privacy is given no explicit constitutional protection, and must be cobbled together via the application of other rights. The United States can be excused for such an omission; at the time that the American Bill of Rights was introduced, personal privacy was more concerned with freedom from unjustified searches or imprisonment than the collection of information. [Lane, 2003] However, Canada's 1982 Charter of Rights and Freedoms also fails to mention 'privacy', a fact which at worst is an intentional exclusion, and at best an unforgivable oversight, given the extent to which other legal bodies had by that time acted to create and protect the individual's 'right' to privacy. By 1890, the United States was examining technology's effect on personal matters – the Warren and Brandeis article, for instance, was describing the potential privacy issues created by cameras in combination with gossip magazines. By the 1930s, the American First Restatement of Torts, which outlines most of that nation's generally accepted principles of law, stated, "a person who reasonably and seriously interferes with another's interest in not having his affairs known to others … is liable to the other" [Lane, 2003], thus providing legal recourse for individuals who felt that they had been improperly exposed. The movement towards privacy protection was certainly not limited to the United States, though; the United Nations' Universal Declaration of Human Rights, adopted in 1948, states in article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence … Everyone has the right to protection of the law against such interference." With such protections in place internationally, and given the clear approach of a highly technological society, it is shameful that Canada did not take a proactive approach to constitutional privacy protection, instead allowing a grab-bag of other rights and laws to define this vital issue.

Regardless of these confusions, a single notion of privacy is needed for this work. Thus, two assumptions will be made. First, it will be assumed that privacy concerns the various degrees of control of all information about oneself, past, present and future. This allows for Alan Westin's four states of privacy to be considered: solitude (control of all information about one's self), intimacy (control of distribution of information, allowing free exchange among intimates, while limiting exposure to outsiders), anonymity (control of one's identity), and reserve (control of one's ideas, though not information about the physical body). [Westin, 1970] By allowing such multiple states to exist, the employee/employer relationship is given space in which to negotiate the privacy minefield. The second assumption that will be made is that privacy is a fundamental human right, as declared by the United Nations. It is foundational to a democratic society: without privacy, there can be no free speech, and without free speech, there is no democracy (while it may be possible to argue this point, it will here be taken as fact). These assumptions do not imply that privacy is inviolate; employers do have the right to protect themselves from liability, and ensure an employee's productivity. However, what is implied is that it should not be assumed that entering into the workplace voids an individual's claim to privacy.

1.2. Definition of Workplace

In addition to examining what is meant by the term privacy, attention must be paid to the changing nature of the workplace. No longer can we concern ourselves solely with the office or the factory floor; the workplace has now extended into homes, public areas and cyberspace. In the 2001 Canadian census, just under 1.2 million people, or 8% of the workforce, reported working at home 3 or more days a week [*Employed Labour Force*, 2004], while in the United States, those who work from home at least once a week make up 15% of the non-agricultural workforce. [*Work at Home, 2005*] Many people are always connected to the office; some 70% of Fortune 100 companies provide their employees with cell phones. [Davidson, 2006] For yet others, particularly those who work at home, connection to the Internet takes place on a company computer, or on company-subsidized web connections. The boundaries of the 'workplace' are virtually limitless, and thus so are those of workplace surveillance. Once an employee accepts a company computer, cell phone, car, etc., the possibility exists that his or her actions will be monitored, even when that person is not using the device for work purposes. The individual becomes employee first, private citizen second, having to be aware at all times of the standards of behaviour set by his or her employer, rather than simply abiding by societal norms.

It is not only the employee who is negatively affected by the extension of the workplace; employer liability also increases. In 2001, Dykes Industries of Little Rock, Arkansas lost a $20.9 million lawsuit filed by a woman struck by a Dykes employee who was talking on a company-provided cell phone while driving. [*Employers Guide*, 2002] Even non-company-provided phones can create liability situations. In 1995, a lawyer in the Florida-based Smith Barney firm ran a red light, striking and killing a motorcyclist. He claimed to have been calling a client, though this was during non-working hours, on his own cell phone, while driving to a non-work-related dinner. Even then, a judge ruled that Smith Barney encouraged their employees to make 'cold calls' to hard to reach clients during non-work periods, and did not warn emplotees of the dangers involved in doing so; the firm was thus liable for its employees' actions while on the phone. The firm settled the case for $500,000. [*Employers Guide*, 2002] Employers may also be responsible for their employees when they are not performing work-related activities; Delta Airlines was found liable in a rape case when a judge ruled that the hotel rooms booked for its flight attendants could be considered a 'work environment.' [Lane, 2003] When the line between on- and off-duty blurs, employers' desire to observe employee actions necessarily increases, in order to protect against costly lawsuits.

Though it is certainly not a wholly positive situation for either side, the workplace has clearly expanded. Thus, privacy in the workplace is not simply concerned with data generated while on company property. It is also concerned with controlling what information an employer can obtain its employees, be that genetic information, the content of e-mails written while working from home, or employees' 'off-duty' choices and activities.

Some time must now be spent in discussing the respective cases presented by employee and employer regarding the issue of workplace privacy. An effort will be made here to assume that neither party is necessarily correct, nor incorrect. The employee will be presupposed to want nothing but fair treatment, while the employer will want a fair day's work. In examining both of these cases it will be hoped that some common ground can be discovered, thus creating potential compromises between employee and employer rights.

1.3. Why Employees Want Privacy

An employee's concern with workplace privacy is not simply a matter of wanting the freedom to do less work. Most employees understand that surveillance is not inherently problematic; if it were designed exclusively to measure output, reward star performers and protect against workplace hazards, it seems unlikely that many objections would be raised. However, employees are generally made to associate monitoring with negative consequences: enforcement of strict rules, stringently defined tasks, punishment for underachievers, etc. Because of this, the desire for privacy becomes more than a longing for extended breaks and freedom from management intrusion. It becomes the desire to be free from medical problems (such as stress, anxiety or depression), to be allowed to be truly productive, rather than machine-measurably productive, and, simply, the desire to be treated as a human being.

Medical Issues

The argument that the removal of privacy protections will only affect those who have something to hide is simply not a valid one. Privacy is a necessity for psychic health, as has been described by many theorists. Alan Westin, for example, writes that there are at least four main psychological functions provided by privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communications. [Westin, 1970] Disruptions of any of these can lead to mental anxiety, which can then manifest itself in physical symptoms.

The workplace is not an exception to this rule. Many studies have confirmed that invasions of privacy lead to higher occurrences of psychological and physical problems. For instance, a joint study between the University of Wisconsin and the Communications Workers of America, conducted in 1990, measured the frequency of occurrence of various symptoms in communications workers, then compared the rate between those workers who were electronically monitored while on duty, and those who weren't. The results were very pronounced. In the group of monitored employees, signs of depression were seen in 81% of individuals; these signs were found in 69% of employees who were not monitored. 72% of monitored workers showed extreme fatigue, as compared with 57% in the non-monitored group. Also, neck problems occurred in 81% of the former group, but only 60% of the latter. [*Stop Snooping*, No Date] This and other studies have made it very clear that employee complaints that workplace privacy violations are stressful are not simply senseless grumblings; there are physical differences to be seen in employees who must endure endless probing, testing and monitoring.

Productivity Issues

It may seem counter-intuitive to speak of employees wanting to ensure productivity; after all, would not most employees be just as happy to produce nothing, so long as they still got paid? This rather cynical view, while not without merit, is an unfortunate situation that has been created by the modern work environment, in which employees and employers are seen to be adversaries. If this circumstance were to change, and workers began to enjoy their jobs and respect their employers, then pride would be taken in the completion of tasks; an employee that feels his or her role is being appropriately valued will be glad to continue to contribute. The main way to achieve these situations is through mutual trust and respect.

Let us consider workplace drug testing. Studies have shown that firms with pre-employment drug tests score 16% lower on standard productivity measures than those who do not test at all. Employers with both pre-employment tests and random testing during employment score 29% lower. The researchers' conclusion: "Companies that relate to employees positively with a high degree of trust are able to obtain more effort and loyalty in return." [Maltby, 1999] Productivity experts tend to agree with this analysis. Tom Peters, who operates a management consulting company, wrote a book analyzing the best-run companies that he had observed. In it, he states, "Treat people as adults. Treat them as partners; treat them with dignity; treat them with respect…. There was hardly a more pervasive theme in the excellent companies than respect for the individual." [Maltby, 1999] Given the right situation, employees will desire productivity just as much as management. Endless monitoring, testing, and regulation of the workplace, though, does not create such a situation.

Humanity Issues

Surveillance does not create better workers; it creates better machines. In 1993, Canada's then-Privacy Commissioner Bruce Phillips wrote in his annual report, "With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for 'corrective' measures." [Phillips, 1993] Workers can be particularly susceptible to such a change, as it is possible to deny them the means to express their humanity. For many positions, work tasks are strictly defined, and deviance from the expected process is not tolerated, thus removing any potential for dynamic thought or action. Electronic surveillance only increases this problem; a 1994 International Labour Organization report on workers' privacy states, "Not only does electronic monitoring have the 'potential' to adversely influence working conditions which have been shown to cause stress, but it may actually create these adverse working conditions, such as paced work, lack of involvement, reduced task variety and clarity, reduced peer social support, reduced supervisory support, fear of job loss, routinised work activities and lack of control over tasks." [*Stop Snooping*, No Date] Employees should not be made to feel that they are easily replaceable machines, free of any uniqueness; by preventing deviance from established norms, the essential humanity of workers is threatened.

It is not only the types of work that employees are asked to perform that can make them feel less than human. A worker loses at least two 'universal human rights' (as defined by the United Nations) when he or she enters the workplace (the right to privacy and the right to peaceable association, as will be described in section 1.6), and he or she arguably loses more than those. Employers are given more freedom to investigate individuals than are law enforcement agencies; in many instances (such as phone tapping, the interception of communications, or surveillance), checks in place to guard against abuses by the latter do not exist for the former. Even outside of the workplace, employers may put limits on actions that are otherwise lawful. It is as if the employment contract somehow alters an individual's legal status; this is something that employees are right to stand up against.

As previously mentioned, workplace privacy is not about laziness. It is about the desire to feel vital to a process, to feel that there is some unique contribution that one can make to the world, and about not losing one's humanity simply by walking through an employer's front door.

1.4. Why Employers Want To Monitor

In response to employee demands for privacy, employers will generally give two main justifications for their various monitoring programs: first, employers have a right to expect an 'honest day's work.' Employees are being paid to produce; there must be a way, then, to ensure that the level of productivity can be monitored. Those who perform their tasks can be rewarded, and those who do not can be corrected; thus, both employee and employer should welcome such programs. The second justification is that an employer has the right to protect his or her assets. That isn't to say that employees are assumed to be thieves – rather, the employer simply wants to be sure that a positive work environment, free from theft, harassment and destruction of valuable resources, is maintained.

In order to examine the above response, five main concerns cited by employers to justify the surveillance of employees will be described: minimizing theft, ensuring productivity, protecting against workplace litigation, avoiding workplace tragedies, and preventing electronic attacks and leaks.

Theft

Theft, both by employees and non-employees, is a very large problem for many companies. A Jack L. Hayes International survey of 27 US retail companies (with sales in excess of $440 billion annually) revealed that those companies lost a staggering $4.7 billion to theft during 2004, with approximately one third of that being done by employees. The survey also finds that 1 in every 28 of the retailers' workers is apprehended for theft, having stolen on average $676 of merchandise. [*Shoplifters*, 2005] Statistics for non-merchandise theft (office supplies, equipment, etc) are more vague, but also seem to indicate billions of dollars in losses for companies each year. Faced with data like this, it is certainly unsurprising that monitoring systems are put in place to

protect company assets. Access and inventory control systems, along with surveillance cameras, are frequently installed to keep an eye on both customer and employee; conveniently enough for companies, cameras installed to watch the former are also able to capture the actions of the latter. In addition to being under constant surveillance, retail workers are also frequently made to undergo searches prior leaving at the end of shift as a further theft prevention measure.

In an office environment, theft of physical objects is not the only problem that must be addressed. Electronic pilfering, such as financial fraud and theft of intellectual property is a rising problem in many companies. A joint Computer Security Institute/US Federal Bureau of Investigations survey found that 9 of 10 respondents were victims of computer security breaches, and of that group, 8 of 10 suffered financial losses as a result. [Lane, 2003] While it would be tempting to blame these attacks on outside individuals, experts have found that 70 to 80% of computer crime is committed by employees against their employers. [Lane, 2003] Thus, companies feel the need to install Internet, e-mail and network monitoring measures, in the hopes of securing their electronic property.

Productivity

An honest day's work for an honest day's pay: this is the mantra of many companies. Unfortunately, this 'honest day's work' is becoming more and more difficult to measure. No longer are employers able to gauge productivity by the number of items generated per day; rather, the workplace is largely shifting into the realm of multi-month projects and customer service, in which employees tend to object to having to their every action measured, claiming that time spent in human-interaction and the development of ideas cannot be regulated as precisely as machine-based work. Scientific Management, or Taylorism, in which every action is measured down to the second, is not an effective tool when evaluating the so-called 'knowledge worker', for whom a day in which no physical output is created can still be considered to be productive. Thus, instead of monitoring employees to ensure maximum periods of productivity, employers attempt to ensure minimal periods of wastefulness. 15 minutes spent in a day handling personal telephone calls and e-mails may be acceptable; 4 hours is not. Multiple ½ hour washroom breaks are also excessive, should they become daily habit. Behaviours such as these can be easily monitored with minimal intrusion. However, closer scrutiny must be given to, for example, longer than average customer interactions, or Instant-Messaging conversations between employees, as it is harder to discern whether or not these actions are wasteful. Because of this need, complex (or intrusive) systems of surveillance become necessary to ensure that a company's best employees are rewarded, and that inefficient employee practices are corrected.

Productivity concerns are also cited in the justification for drug, health and/or genetic testing. An employee who comes to the workplace drunk or on drugs will not be able to perform his or her job effectively or safely. An unhealthy employee may become less physically capable of completing his or her duties, or require longer sick leaves. A person with a genetic propensity for a disease associated with a certain workplace environment may not be the individual best suited to that position. By testing employees

during the hiring process, or occasionally throughout their period of employment, companies are able to better ensure productivity, safety and job suitability.

Protection Against Litigation

In 1995, an e-mail entitled "25 Reasons Why Beer is Better Than Women" circulated around the Chevron corporation's computer systems. A number of female workers subsequently sued the company for creating a hostile work environment, introducing the e-mail as evidence. Chevron lost the case, and was ordered to pay out over $2.2 million. [Lane, 2003] In March 2006, the US Equal Employment Opportunities Commission (EEOC) settled a $2 million lawsuit against 3 Cracker Barrel restaurants accused of racial and sexual harassment, accusations ignored by the restaurants' managers. In fact, the EEOC reports that in total, $107.7 million was recovered from companies in various harassment suits in 2005 (down from $168.1 million in 2004) [*EEOC Litigation*, 2006], after having received over 23000 sexually- and 26000 racially-based complaints. [*EEOC Charge*, 2006] Many of these suits result from accusations of management indifference, in which plaintiffs claim that a company had every opportunity to identify and control problematic individuals, but did not do so. Harassment is not the only area in which companies must protect themselves, however. As was described above in the expanding nature of the workplace, businesses can also be held responsible for the negligence of employees while on duty – a term that's meaning broadens with each passing year. Employers are thus led to feel that they must fully monitor workplace conditions and events, lest they become liable for the negative actions of their employees.

Workplace Tragedies

One of the most unfortunate realities facing both employees and employers in the modern workforce is workplace violence. A US Bureau of Labor Statistics census reported that in 2004, 551 workplace homicides occurred, a number actually below the 1999-2003 average of 642. [*Fatal*, 2005] This means that on the average workweek in the United States from 1999 to 2004, between 10 and 12 employees died as the result of an attack. We must not think, however, that this is a uniquely American issue: in British Columbia alone, over 10 000 acts of on-the-job violence were reported between 1997 and 2004. [*Occupational Injuries*, no date] Employers of course have every reason to want to protect their employees, as an unsafe work environment will naturally drive down production as well as hasten the departure of many workers (not to mention more humane issues). Recently, though, an additional pressure has been placed on companies: lawyers, realizing that companies have deeper pockets (or better insurance) than individual perpetrators, have devised methods of holding employers responsible for workplace deaths, from allegations of negligent hiring to negligent retention of employees. Employers are thus being advised to perform thorough background checks on new hires, as well as periodic personality evaluations, in attempts to identify any potential dangers prior to the occurrence of a violent incident. [Lane, 2003] Companies are then left with a conundrum: they can monitor all workers, potentially creating an atmosphere of unease, or they can selectively monitor individuals, and risk not properly anticipating an incident or face accusations of profiling. In this lose-lose situation, employers are left to

grudgingly select the former option, protecting both their employees and themselves at a cost of potential privacy violations.

Electronic Attacks and Leaks

The final reason cited by employers for the need to monitor workers is the very real threat of damage to electronic records. Before 9/11, the greatest fear of attack in North America came from cyberterrorism – the Rand Corporation, for example, warned of the potential of a "digital Pearl Harbour." [Lane, 2003] No longer must an employee use accelerant and flame to destroy records; a single well-written virus or theft of a hard drive can cause millions of dollars worth of damage. The increasingly electronic nature of corporate records also creates greater potential for leaks. Employees have the ability to, intentionally or otherwise, release to the public confidential memos or million-dollar trade secrets with the click of a mouse. Non-disclosure agreements provide employers some legal recourse should such a leak occur, but information, once released, is virtually impossible to reclaim. The leak of, or damage to, confidential or vital information has the potential to destroy a company; it is not at all surprising or unreasonable, then, that employers would want to routinely monitor all access, electronic or physical, to their holdings.

1.5. Situations in Which Privacy Conflicts May Arise

As has been described, employees and employers frequently view matters of privacy from different angles. Stressed-out employees feel that they are being forced to give up basic human rights for the 'privilege' of working, with no recourse. Aggravated employers read statistics such as "on average, men spend 4 hours a day checking the Internet" [*Internet Use,* 2005], and wonder how employees can possibly object to measures designed to ensure safety and productivity, while minimizing losses. Perhaps, if situations in which workplace privacy issues arose were rare, trade-offs could be reached, without the need to ever address the true roots of the problem. This, of course, is not the case, though. Workplace privacy issues arise throughout the entirety of the employment relationship, from pre-employment background checks to on-the-job monitoring to control of off-duty activities. In this section, some of the various situations in which privacy issues manifest themselves are examined.

Pre-Employment

Pre-employment testing has become a very large industry. A quick glance through Lester Rosen's "The Safe Hiring Manual: The Complete Guide to Keeping Criminals, Imposters and Terrorists Out of the Workplace" [Rosen, 2004] shows why this is true. It describes the importance of pre-screening in the US, the ways in which pre-screening shows due diligence in case of negligent hiring lawsuits, the legal use of criminal records, the proper administration of drug and personality tests, how to uncover embezzlers, and the ways to skirt state and federal laws in order to make these inquiries (and many, many others) legal. No longer is the only goal of an employer to hire the right candidate for the job; rather, it is increasingly the case that companies also want to hire the person least likely

to expose them to liability, cost them large sums in worker's compensation claims, or challenge workplace conditions in court. [Lane, 2003] Thus, background checks become more thorough, personality tests more probative, and genetic tests more frequent.

Naturally, this creates a minefield of privacy concerns. There is currently little to no protection for individuals who refuse to co-operate in these procedures; an applicant who does not allow an employer to perform a credit check, for example, is offered no legal recourse should he or she be summarily rejected because of this denial. Though bills such as the US's Genetic Non-Discrimination Act have been introduced (but not passed), and the Canadian Privacy Commissioners have been calling for the ban of pre-employment genetic tests for over a decade (e.g. [Wright, 1993]), applicants may still face challenges should they be shown to have a higher probability of developing a costly medical condition, have previous legal problems, or a prior history of filing complaints against his or her employers. By digging deep enough into the virtually all areas of an applicant, employers can usually find a flaw, which they are then permitted to treat as they see fit. Unfortunately, there is no clear point at which such testing moves from the realm of due diligence and into privacy violation or discrimination.

Drug Testing

Once a person has been hired, the testing process does not stop, as random drug tests are often administered. Justification of this practice frequently comes from a 1972 study by the Firestone Tire and Rubber company, which asserted that drug users have 2.5 times more absences than the average worker, are 3.6 times more likely to be involved in a workplace incident, 5 times more likely to file worker compensation claims, and 3 times as likely to use health care benefits (this of course ignores that there actually was no Firestone study, and that these unsubstantiated figures were only mentioned at a company luncheon, then spread as fact). [Maltby, 1999] Naturally, employers who see these statistics cited in research papers want to reduce these occurrences within their own staffs, and introduce drug-testing programs to do so. An impaired employee is naturally both a dangerous and unproductive employee, it is thought, and thus tests for substance abuse become necessary.

Drug testing, though, is extremely invasive, often inaccurate in strange ways, and ineffective. Any drug test involves obtaining a physical sample of a person, be it blood, urine, hair or saliva, thus making such tests the most physically invasive of any of the privacy-threats discussed in this report. This invasiveness is not justified by results, though. While the rate of false positives can be reduced by proper testing conditions and re-tests of initial positive results, certain products can still confuse urinalysis tests: codeine, for example, produces the exact same drug metabolite as heroin; poppy seeds create morphine metabolites; hemp oil products mimic THC (the 'active agent' of marijuana). [Maltby, 1999] Another, rather ironic, system failure is that random drug tests (particularly urinalysis) will often fail to detect on-the-job drug use, as metabolization may take hours to occur. Hair testing can also be a contentious issue, as all else being equal, residue in dark hair will be detected more easily than in light hair, and absent of differences in drug use, African-Americans are more likely to test positive

than Caucasians. [Maltby, 1999] Finally, the fact that a person has tested positive for drug use does not necessarily imply that they are currently impaired. Hair analysis, for instance, can show drug use months prior, while urinalysis often finds metabolites days after a drug's consumption. The assumption that past drug users will inevitably consume a particular substance in close enough proximity to the workplace to affect their performance is simply false. A 1994 US National Academy of Sciences study found that, "the data … do not provide clear evidence of the deleterious effects of drugs *other than alcohol* on safety and other job performance." [Normand, 1994]

Because of its invasiveness into not only a worker's body, but also his or her off-duty lifestyle choices, drug testing is a very contentious issue. While alcohol tests (such as the breathalyzer) may be a reasonable precaution for safety-critical positions, as they test for *current* impairment, drug testing does not necessarily do so. Thus, a company is left with a choice: ignore statistics and only do the amount of testing that is absolutely necessary, or test all employees for drug use and risk losing highly qualified employees (due to positive tests or moral objections to the tests themselves). More and more companies are beginning to choose the former option – in 1996, 81% of companies surveyed by the American Management Association (AMA) tested employees for illegal substances; by 2004, that number had dropped to 62%. [*2004 AMA*, 2004]

Medical Testing

Medical testing programs, such as genetic screening, pregnancy tests, AIDS/HIV tests, etc., pose somewhat different workplace privacy questions than drug testing, though the procedures are very similar. Where drug tests reveal lifestyle choices (which, at least in theory, are optional), medical tests uncover intimate and sometimes innate aspects of a person's body. It is even possible that such tests will reveal information that the individual does not yet know, and may not want to know. The results of these assessments, which are generally stored by the employer (or on a medical record to which the employer has access), can be devastating to a person's life if revealed; even in 2006, a leaked positive test for HIV, for example, can alienate an individual from his or her entire community. However, without medical testing, an employer may not be able to identify an increased susceptibility to workplace hazards, or even evaluate an individual's fitness for duty. The employer's desire to maintain a safe work environment must thus be balanced with the employee's right to privacy.

The 2004 AMA Workplace Medical Testing Survey [*2004 AMA*, 2004] revealed that in general, companies recognize the need to limit testing to that which is necessary to ensure job safety. While 46.5% of employers test for fitness for duty, only 2% test for HIV. Increased susceptibility to workplace hazards is tested for by 15.1% of employers; 2.8% check for STDs. Further, only 0.8% of companies use HIV test results in decisions about retaining/dismissing employees, and only 1% use STD status for that purpose. Even in hiring decisions, information such as family medical history is only used by 3.8% of employers. Those who do perform extensive testing are limited in the ways in which they can use any information they collect; the Americans with Disabilities Act, for instance, says that if an person is rejected for work on the basis of a medical test, the

employer must prove that it would be physically impossible for that individual to do the work required. [*How Private*, 2006]

In the end, medical testing done properly does not have to be a privacy risk. Properly conducted, well-justified tests should not raise the ire of most employees, and appropriate safeguards in the handling and storage of test data will protect against potentially devastating leaks of highly confidential information. That being said, companies absolutely cannot assume that an individual knows beforehand what the results of any particular test might be, or that he or she wants to know or is better off knowing them. The individual's right to privacy must be particularly enforced in this situation, as medical information is among the most sensitive aspects of a person.

Continuous Electronic Monitoring

When the issue of 'privacy in the workplace' is raised, it most often refers to the widespread practice of continuously electronically monitoring employees. There are a myriad of ways in which this is done: video cameras record the physical actions of employees, while Internet monitoring software and keystroke loggers keep tabs on those performed online; e-mail is read, Instant Messaging programs are scrutinized and telephone conversations are recorded in order to examine communications; the Global Positioning System (GPS) is used to track company cars, cell phones or ID badges; RFID-based door access systems collect information on employees as they traverse the workplace; and biometric systems are employed to confirm identity for access to resources. Any or all of these measures, along with many others, can be taken by an employer to ensure productivity and protect resources, tasks that become more difficult and costly as the workplace becomes larger, non-centralized and more electronically focused. Systems such as those listed above are turned to when employee output cannot easily be measured (as is the case in many office environments), and when the price of installing and operating such a system drops to a level of apparently certain cost-effectiveness. Judging by usage statistics, one or more of those criteria are frequently being met. According to the AMA's 2005 Electronic Monitoring & Surveillance survey, 76% of companies monitor Internet connections, 55% retain and review e-mail messages, 51% track employee phone usage (up from just 9% in 2001), 51% employ video surveillance (up from 33%), up to 8% use GPS to monitor cell phone, vehicle or ID badge location, and 53% make use of SmartCard access technology. [*2005 Electronic Monitoring*, 2005] Additionally, it should be noted that electronic surveillance is not used idly: fully 1 in 4 companies have terminated employees for improper Internet use, and the same number have fired workers for misuse of e-mail. [*2005 Electronic Monitoring*, 2005]

An outraged employee has valid arguments as to why such practices should not be allowed, at least not in the unhindered form in which they currently exist. First, the act of entering the workplace should not strip one of his or her human rights; acts that outside the office would be considered felonies (electronic interception of communications, for example) should not be considered appropriate and justified for a company; this, however, is not the case. Neither the RCMP nor the FBI has the same freedoms to

monitor individuals as the chief security officer of a corporation. Law enforcement agencies must justify video surveillance, wire-tapping or tracking technologies to a judge; companies are generally free to utilize them as seen fit. Further, 1 in 5 U.S. companies did not inform employees of surveillance measures, as in many jurisdictions (including 7 Canadian provinces) there is no law requiring employers to do so. [*2005 Electronic Monitoring*, 2005] A second issue that can be raised by an employee about electronic surveillance concerns its effectiveness. As previously stated, constant monitoring of employees is very stressful, and negatively effects worker morale, and may thus actually lead to a decrease in productivity. Does it truly matter that a person spent an hour online, so long as the necessary amount of work was accomplished? If productivity is difficult to measure, is 'time spent not on task' truly a measure of anti-productivity, particularly for so-called 'knowledge workers'? And if liability is the issue being addressed, could it not be reduced through education, rather than universal suspicion? An employee should be able to expect that each of these questions be readily answered each time a new surveillance method is deployed.

Constant electronic surveillance is at the heart of modern workplace privacy issues; it forces an examination of the balance between the employer's right to protect business interests and the employee's right to be treated as a human within his or her workplace. Given the current state of workplace privacy, it would seem that the lack of legal protections for employee privacy has tipped the scales to the former interest.

Off-Duty Surveillance

As has been previously discussed, employees are finding that it is more and more difficult to truly be 'off-duty.' This does not mean, though, that once an individual has achieved such a state that they are free from the watchful eye of his or her employer. For instance, in 2005, there were at least two reported cases of brewery employees being fired because they were spotted drinking a competitor's beer. The first involved Isac Aguero, a forklift operator for a Miller Brewing distributor. A photo of him holding a Bud Light (brewed by Miller competitor Anheuser-Busch), taken on a Saturday and including no identification of him as a Miller employee, was displayed in a local newspaper. The day that the picture ran, Aguero was called into his supervisor's office and told that his four-year employment with the company was being terminated – no reason was given, but the implication was that the photo was considered unacceptable. [*Beer*, 2005] Three months later, the story of Ross Hopkins, an employee of a Colorado-based Budweiser distributor, appeared. Hopkins had filed suit alleging that he was fired when the son-in-law of the distributor's owner spotted him drinking a Coors. While Colorado law states that workers cannot be fired for legal, off-duty activities, it provides exceptions in cases of conflicts of interest. Lawyers for the distributor argue that this case is such an exception, as Hopkins was wearing his Budweiser uniform while drinking the Coors, creating at least the appearance of a conflict, particularly because they claim he was also making disparaging comments about Budweiser beer. [Sarche, 2005]

Incidents such as these raise a final, and very real, privacy conflict. Employers feel that they must protect the image of their product at all times, and that detrimental employee

conduct, even while off-duty, can reflect poorly on the company. Companies also cite matters of insurance and absenteeism, which (it is argued) increase in individuals who smoke, are overweight, or who participate in 'dangerous' activities such as skydiving or rock-climbing. Employees, on the other hand, argue that off-work time is just that: time in which the individual is completely disconnected from his or her employer. It is during this period that an individual should be able to speak his or her mind freely and without fear of reprisal, and to unwind from the working day with any activity, and certainly at least any legal activity, without needing to obtain his or her company's permission. Limitations of off-duty actions are a slippery slope: if an employee cannot publicly disparage his or her employer while on duty, can they do so while off-duty, but still wearing an identifying uniform? Or at an establishment in which the majority of the other patrons know by whom he or she is employed? Or while with friends, who could spread information as coming from 'someone in the know'? Once an company is allowed control of some set of off-work activities, it can only be expected that it will attempt to expand this arrangement.

In this case, the laws that exist tend to favour employee rights. In the United States, for instance, approximately half the states have laws preventing employers from firing workers who smoke while off-duty. [Armour and Appleby, 2005] Also, California, Colorado and North Dakota have laws that protect employees from being fired for legal, off-duty activities. [Lane, 2003] Regulations such as these, though, are just a first step. Comprehensive definitions of what activities can and cannot be limited by an employer must be developed in order for employees and employers to both understand the nature of off-duty surveillance.

1.6. Small Incidents with Large Consequences

In this section, two specific workplace privacy incidents will be examined. Neither received a great amount of publicity, though their implications could be quite great. Also, neither is Canadian – a fact that will be discussed later in the paper, as it only exemplifies the fact that so much of the workplace privacy information available is not native to this country. They are small incidents, but with potentially large consequences for continuous electronic monitoring and off-duty surveillance in particular, but also for the balance of power between employee rights and an employer's right to protect its interests.

The VeriChip

In February 2006, a Cincinnati based video surveillance company announced that it would be adopting a new layer of security for its data centre: VeriGuard, an access control system based on the VeriChip, a glass-encased RFID tag the size of a grain of rice, which is implanted in the triceps area of a person's arm, and is readable at a distance of a few inches. Though reports differed as to whether or not this implant would be mandatory for employees who wished to enter the data centre [Zwirn, 2006; Libbenga, 2006], it is certain that at least two employees underwent the procedure. Though the

VeriChip has long been marketed as (among other things) a tool for access control, it was believed that this was the first instance of such a use in the United States.

It was not, however, the first such global use of the VeriChip in humans. In 2004, the Mexican Attorney General and 160 members of his staff 'got chipped' in order to control access to secure areas, as well as to serve as an anti-kidnapping tool. Two European bars, the Baja Beach Club in Barcelona and Bar Soba in Glasgow, offer VIP privileges to patrons willing to have the chips implanted. The U.S. Food and Drug Administration has also approved the VeriChip's use for medical record retrieval; former US secretary of Health and Human Services Tommy Thompson (who is also on the VeriChip Corp. board of directors) has very publicly announced that he intends to have the chip implanted for this purpose.

Instances such as these appear to be harmless. With the exception of the Mexican Attorney General's staff, all of the individuals who have had a VeriChip implanted have volunteered to do so. Again with the exception of the Mexican case, each of these individuals was given truthful information about the uses of the VeriChip (the Mexican Attorney General's staff was outright lied to when it was sold the VeriChip as an anti-kidnapping tool; the read range is not large enough to do anything but identify an individual, not track one, assuming the chip is not removed by a kidnapper), though potential privacy concerns may not have been addressed. Finally, due to the relative rarity of VeriChip readers, it is currently highly unlikely that any chip will be surreptitiously read.

What, then, are the threats to workplace privacy? They come when the circumstances making the VeriChip 'harmless' begin to change. It is very possible, even likely, that VeriChips will not remain optional for many employees. Should this technology prove itself useful in small test cases, a push will inevitably be made for its expansion. This will not require a change in the legal climate. Most current privacy law, as will be discussed below, is based on the 'reasonable person principle'; that is, a technology is legally acceptable if a reasonable person would find it to be appropriate under the given circumstances. It is likely that once the VeriChip has proven itself secure, employees at some ultra-high security workplace, such as a nuclear power plant, will be 'asked' to have the chips inserted; those who refuse will be re-assigned (or have their employment terminated) – upon any potential legal challenge, this will likely be deemed a 'reasonable' security measure. Simultaneous to this development, chips used for quick access to medical records will become more popular (particularly as stories are published of unconscious individuals being treated properly only due to the availability of their VeriChip-indexed medical records). From there, we have a slippery slope. With the current fears of terrorism, airline workers are put under increased scrutiny; perhaps the VeriChip will be the best way to ensure that their credentials are legitimate, and cannot be stolen. US Government employees already must carry RFID tags at all times; the VeriChip would ensure that secure areas remain so. As the chip becomes more and more widely used, the situations in which the chip is accepted as 'reasonable' will broaden, a cycle which will continue until all objections are quashed.

Perhaps this scenario is a simple flight of fancy. However, it should not be dismissed out of hand. As previously stated, the current uses of the VeriChip can be considered harmless; this will inevitably speed its adoption. Moreover, if a major privacy threat occurs, it will occur when the technology is widespread – and thus embedded in society. Incidents will likely not occur if only one in ten thousand people carry the chip; at that point, the only readers deployed will be those used for the initial purposes. If one in a thousand people have them, though, readers will become more prevalent (and less expensive), thus allowing more services to be offered – implantable RFID chips may become a benchmark of convenience, a state that would drastically increase the technology's adoption rate – and overcome public perceptions of the chip's 'creepiness.' It will only be at this time, when the chip has become pervasive, that a major privacy threat is likely to arise, as it is then that an attack would be most profitable. However, if the VeriChip offers enough convenience (or safety) to users, this threat will be taken as an acceptable risk.

Tens of millions of pets, and an equal number of livestock, already carry RFID implants. [Lockton, 2005] Should this level of adoption be seen for humans, what happens to workplace privacy? Employees can be physically tracked with a device they cannot remove, as at very least readers can be installed in every doorway in a building; health records will be instantly available to employers, along with any other records attached to the chip (assuming the same chip will be used for door access and health record indexing); off-duty monitoring will be increased as non-work related chip reads will need to query the VeriChip-controlled database; essentially, all aspects of employee privacy will be reduced (or eliminated). All of this can occur simply due to a grain-of-rice-sized chip, and a lack of proactive privacy laws.

Guardsmark vs. Fraternization

The second incident that will be described does not require nearly the same futuristic approach as was taken with the first; the results of this incident can be seen immediately.

In 2005, the US National Labor Relations Board dealt a great blow to fundamental workplace protections. The issue being reviewed was a rule instituted by Guardsmark, a security firm, that stated that employees were not permitted to "fraternize on duty or off duty, date, or become overly friendly with the client's employees or with co-workers." [*Big Brother*, 2005] In a 2-to-1 decision, the Board ruled that the regulation was lawful, as the members felt that Guardsmark employees would interpret it as a simple ban on dating. The dissenting member, however, noted that dating was explicitly mentioned in the rule, and thus the workers would interpret the term 'fraternize' to mean something else. The primary definition of the term, she added, is to, "'associate in a brotherly manner' … and that kind of association is the essence of workplace solidarity." [*Big Brother*, 2005]

A rule that bans off-duty fraternization between employees may seem extreme, but it is only a small step beyond regulations that are already commonplace. The US National Labor Relations Act, for instance, allows employers to ban association between

employees during work hours. Many companies have rules in place that seek to control workplace romances (in order to avoid sexual harassment lawsuits); Wal-Mart, for instance, insists that any employees who wish to date must first get the permission of their supervisors. [Lane, 2003] This policy was challenged in New York State on the basis that dating was a legal recreational activity, and was thus protected under state law; the appellate court, though, ruled that dating does not constitute a 'recreation', at least under the terms of the statute. [Lane, 2003] Thus, employees can be prohibited from associating while on duty, and can be banned from dating while off-duty (a rather vague rule; after all, a fun night out to one person may be a date to another); is it any surprise that all on- and off-duty fraternization can thus be stopped?

If the answer to the previous question is 'no', then workplace privacy has taken a substantial hit, for various reasons. To begin, one of the greatest protections for employee rights is the presence of trade unions. Both in Canada and the United States, workers are guaranteed the right to join such a union, should they choose to do so (by the Canada Labour Code and the US National Labor Relations Act, respectively). When fraternization between employees is banned, however, this becomes extremely difficult. Employers are not required to inform employees of their right to associate with co-workers for collective bargaining or other such purposes, and thus with few exceptions do not. With so much of the workforce working in an 'at will' capacity (that is, they can be fired for any or no reason, short of discrimination), how can an employee be expected to risk his or her job simply in order to discuss unionization? When anti-fraternization rules are allowed to stand, the privacy protections of organized labour are eradicated.

Furthermore, in both Canada and the United States, as well as many other countries, the freedom of peaceable assembly is constitutionally protected. Can a workplace rule truly extend so far as to affect an individual's Charter rights? When a person is on duty, the answer is a clear 'yes'; however, the off-duty employee has generally been protected. For the National Labor Relations Board to allow a rule preventing employees for gathering for an after-work drink, it is ludicrous. It implies that the workplace has no boundaries; that there is virtually no limit to the allowable attacks on employee privacy. Once an employee's off-duty associations can be controlled, what else could follow? This is a question that will be left to the reader to ponder.

The VeriChip and anti-fraternization rules are but two instances in which workplace privacy is under attack. While employers have not yet been given *carte blanche* to fully monitor employees' actions, such a time seems to be approaching. Fortunately, some efforts are being made to limit workplace surveillance, and to protect the privacy of the employee. They are not yet close to comprehensive, but they are a start. In the next section of this paper, the privacy laws of Canada and others will be examined, so that we can begin to address the work that must still be done.

2. APPLICABLE LAWS

2.1. Federal - PIPEDA and the Privacy Act

There are two federal privacy laws in effect in Canada: the *Privacy Act*, and the *Protection of Personal Information and Electronic Documents Act* (PIPEDA). The *Privacy Act* preceded PIPEDA, taking effect in July of 1983. It regulated the collection, storage and disclosure of personal information by 150 different federal agencies and departments, and gave individuals the right to access and request correction to any information on them collected by a federal agency. This Act will be discussed only minimally in this paper, as it tends not to be cited in workplace privacy cases. However, the phrasing of the legislation should be noted. The basic principle for collection that must be followed reads: "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of an institution." The collection of employee personal information is thus allowed (within prescribed limits), if the institution can show that it is necessary to manage him or her (and is thus vital for the operation of the institution).

However, PIPEDA will be vital to this discussion. Introduced partially in 2001 (for federally regulated private-sector organizations, such as banks, airlines, or telecommunications companies), and fully in 2004 (for provincially-regulated organizations, such as retailers, manufacturers or the service industry), this act applies to the collection, use and disclosure of information from commercial activities of any organization, as well the personal information of the employees of federally regulated private-sector organization. It does *not*, importantly, apply to employee personal information for provincially regulated businesses. [*Privacy*, 2004] In PIPEDA, a number of principles for the collection of data are outlined, based on the Canadian Standards Association's *Model Privacy Code*. These principles include, for instance, mandates to:

- identify the purposes of collection, and inform those whose information is being collected of these purposes before or at the time of collection;
- obtain consent from individuals before collecting personal information;
- limit collection to that which is necessary for the purposes identified;
- limit disclosure and use of information to the purposes identified;
- and ensure the accuracy of and provide safeguards for information collected.

There are two main clauses of PIPEDA that will be of interest to this discussion, in addition to the mandates listed above. The first is section 5(3), which reads: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances." This restriction will be referred to frequently in this paper. The 'reasonable person' test adds a degree if subjectivity to the law; it is left up to corporations, judges or the Privacy Commissioner of Canada to argue what exactly is considered 'reasonable', an argument that can be found in many PIPEDA-based complaints. The second clause that deserves consideration is that allowing conditional collection of personal information without consent. Section 7(1)(b) reads:

> [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 relating to investigating a breech of an agreement or a contravention of the laws of Canada or a province.

A similar exception applies to the use of personal information without knowledge or consent. Section 7(2)(a):

> [An organization may use personal information without the knowledge or consent of the individual only if] in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of a law of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention.

Thus, employers subject to PIPEDA are allowed exceptions to ethical data collection principles if they are investigating a breech of contract (including the employment contract) or an illegal activity; when facing accusations of wrongful collection of personal information, companies frequently cite this exception. Similarly, the latter exception is cited in at least one case that will be discussed, in which an employee accused his employer of wrongfully using his personal information.

If an individual feels that his or her PIPEDA rights are being violated by an organization, he or she can file a complaint with the Privacy Commissioner. While this is an important measure to have in place, there are weaknesses in the system. First, the Commissioner has no remedial powers; rather, he or she issues a report on the matter, classifying the complaint as *well-founded, not well-founded,* or *resolved*, and issues recommendations, if any are applicable. Should the applicant not be satisfied, he or she may proceed to the Federal Court, which is able to enforce compliance and award damages. A rather important second weakness in PIPEDA, in addition to the lengthy process needed to insist upon its observation, is that fact that in published reports, the Privacy Commissioner cannot reveal the identity of the complainant nor the defendant. While this does provide a measure of protection for individuals, it also allows for greater abuse of data collection principles by companies. If a company were to be identified as mishandling employee (or customer) personal information, public action (such as a boycott) could be taken. As it is, a company is free to violate PIPEDA until a complaint has been filed; if the company then changes its policy, its name will never be released to the public (excepting if the applicant chooses to sue for damages).

These weaknesses, as well as the fact that employees of non-federally regulated organizations are given no protection, aside, PIPEDA has done more to protect Canadian workplace privacy than any other federal law.

2.2. Provincial

At the provincial level, it can been noted that every province has legislation governing the collection, use and disclosure of information held by government agencies, each of

which is largely similar to the federal *Privacy Act*. Some sector privacy protections also exist, protecting for instance records held by financial institutions (the federal *Bank Act*), or health records collected by practitioners and other health care organizations (regulated in Alberta, Saskatchewan, Manitoba and Ontario), but in general employees are left to fend for themselves when it comes to private-sector workplace privacy. Provinces are thus forced to pass legislation that is 'substantially similar' to PIPEDA, in order to protect private-sector employees. Three provinces have done so: Quebec (whose privacy laws were in force prior to the introduction of PIPEDA), Alberta and British Columbia.

BC/Alberta PIPA

The Personal Information Protection Act (PIPA) of both British Columbia and Alberta are nearly identical (as they were developed at the same time, and by the same group), and thus will be treated together. Both have been ruled substantially similar to PIPEDA, and thus supercede it in their respective provinces. However, there are two main differences between the PIPAs and PIPEDA that are of significance to this discussion. First, the PIPAs are not restricted to public works; they apply instead to "all organizations." Thus, companies in the private sector in both Alberta and BC cannot collect employee personal information without reason or justification; all the standards of reasonable collection, use and disclosure provided by PIPEDA for public sector employees are in force.

Secondly, an interesting clause in both PIPAs concerns the collection, use and disclosure, without consent, of employee personal data, essentially stating that consent is not required for reasonable collection of information, so long as notification is given. The BC PIPA, for instance, reads in part;

> Collection of employee personal information
> 13(1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual.
>
> (2) An organization may not collect employee personal information without the consent of the individual unless
>
> …
>
> (b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.
>
> (3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the personal information without the consent of the individual.

Workplace privacy in Alberta and BC is thus held at lower importance than general individual privacy. While it is encouraging that notification was made mandatory, the fact remains that this clause weakens employee rights.

Quebec

The third piece of legislation ruled to be 'substantially similar' to PIPEDA is Quebec's *Act Respecting the Protection of Personal Information in the Private Sector (the Act).* While there is not enough difference between the *Act* and PIPEDA as to necessitate an additional examination of any clauses, the foundation of the Act is very significant to this discussion. Where PIPEDA and PIPA in BC and Alberta work to establish privacy rights for individuals, this *Act* is simply confirming rights set out in the *Civil Code of Quebec,* which in part reads as follows:

> Chapter III – Respect of Reputation and Property
>
> 35. Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person unless authorized by law.
> 36. The following acts, in particular, may be considered as invasions of the privacy of a person:
>
> …
> 2) intentionally intercepting or using his personal communications;
> …
> 4) keeping his private life under observation by any means;
> …
> 6) using his correspondence, manuscripts or other personal documents.
>
> 37. Every person who establishes a file on another person shall have a legitimate reason for doing so. He may gather only information which is relevant to the stated objective, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or damage the reputation of the person concerned.

The *Quebec Charter of Rights and Freedoms* also notes that, "Every person has a right to respect for his private life." That is, the *Quebec Charter* establishes a right to privacy that is missing in the *Canadian Charter of Rights and Freedoms*, though the latter was written less than a decade prior. The citizens of Quebec were wholly unaffected by the introduction of PIPEDA (save for inter-provincial data exchange), and in fact are given greater privacy protection than any other province (note that as opposed to Alberta and BC, Quebec does not provide an exception to consent for collection of employee personal information). To see this, we can look at collective bargaining agreements in that province. For instance, an agreement between the *Journal de Montréal* and its unions requires that all surveillance be conducted with respect to the *Charter*. [Kiss and Mosco, 2005] The question begs to be asked, then: why are privacy rights not constitutionally protected in the rest of Canada?

2.3. United States

In the United States, workplace privacy protection becomes harder to define. There are few laws relating directly to this issue; instead, worker rights are cobbled together from a variety of other protections. As previously mentioned, privacy itself is not constitutionally protected; rather, it is inferred from other articles of the Bill of Rights. Thus, employees (or their lawyers) are forced to pour through the annals of American legislation, in hopes that some privacy protection can be found.

There are situations, of course, that are well known to be protected. Title VII of the *Civil Rights Act* of 1964, for example, already prohibits some pre-employment inquiries. In order to remove the discrimination that was rampant in the 1960's workplace, employers may not discriminate (and thus may not question during interviews) based on religion, race or national origin. [Unfortunately, a series of events has also led this Act to result in an increase of workplace surveillance, as employers attempt to eliminate sexual harassment (which has been ruled to be discriminatory) from the office.] Under the *Fair Credit Reporting Act*, an employee (or job applicant) must give separate, unequivocal permission for a company to access his or her credit report (though, should he or she refuse to do so, his or her chances at getting or keeping a job will severely decrease). [Lane, 2003] The *Employee Polygraph Protection Act* protects employees from being subjected to lie detector tests in most situations. Also, the *Americans with Disabilities Act* will occasionally, but not always, either prevent random drug tests or see that those who test positive are not summarily dismissed.

In general, U.S. laws support the power of management to abrogate the privacy rights of employees. [Rosenberg, 2005] Even when attempts are made to control this trend, failures frequently occur. The *Electronic Communications Privacy Act* was passed by Congress when it was belatedly realized that technology was allowing employers to routinely monitor phone conversations and other forms of communications. [Lane, 2003] The basics of the law are straightforward; it is illegal to intercept electronic communications while in transit. The final two words are a vital weakness, however, as e-mail messages, for instance, are rarely 'in transit.' The *ECPA* also does not apply to service providers – a status that applies to most companies. Thus, the *Act* that was written to prevent the monitoring of employee communications essentially does not apply in the workplace. [Rosenberg, 2005]

Laws that are unequivocally supportive of workplace rights tend not to be passed. For instance, in 2004 supporters of workplace privacy were given a small measure of hope when the California Assembly passed Senate Bill 1841, which would have required employers to "inform employees if job site e-mail and Internet activities are being monitored." Such a law would have required nothing more than a "one-time written notice if [employers] plan read e-mail, track Internet use, or use other electronic devices to monitor employees on and off the job." The bill went to the Senate, and then to Governor Arnold Schwarzenneger – who promptly vetoed it, saying that, "for business purposes, employers should have the ability to monitor employee activity in order to ensure that (Internet and e-mail) access is not being abused" (seemingly ignoring the fact

that the bill did not seek to limit such monitoring, merely inform employees of its existence). In the United States, it would seem, even small concessions to workplace privacy will not be granted.

What Might Have Been

"For of all sad words of tongue or pen, The saddest are these: 'It might have been.'" [Whittier, 1856] Though John Whittier was speaking of love when he wrote these words, they remain appropriate when considering 'what might have been' for American workplace privacy law. Consider, for instance, the *Privacy for Consumers and Workers Act*, introduced in 1992. Had this bill been approved, employers would have been required to:

- Clearly define their privacy policies;
- Notify prospective employees of electronic monitoring that might affect them;
- Limit surveillance to ensuring job performance;
- Refrain from monitoring personal communications;
- Give employees access to any information about them collected during surveillance;
- Refrain from video monitoring in locker rooms and toilets; and,
- Notify workers when telephone monitoring was taking place. [Lane, 2003]

This bill, one might think, does not put too high a burden on employers; it simply provides that notification of surveillance be given, and that monitoring be well-defined. This, of course, was not the opinion of many employers. Various business organizations, from the Household Finance Corp. to the Associated Builders and Contractors complained that this new bill would limit their ability to videotape striking workers. The vice-president of the National Association of Manufacturers also stated that, "random and periodic silent monitoring is a very important management tool." He went on to deliver the rather novel 'stage fright' objection, in which he argued that employees actually function better when they don't know they're being observed, and that this bill would thus increase stress in the workplace. [Lane, 2003] The bill never got past Congress.

A simpler bill, involving simply the notification of employees in cases of electronic monitoring, was also summarily rejected. Under the *Notice of Electronic Monitoring Act*, employers would have been subject to civil liability should they fail to provide employees with proper notice of electronic surveillance, including the type of monitoring, the means of monitoring, the information to be collected, how it would be used, and the period of surveillance. This bill, though, failed both of its introductions, once in the House of Representatives and once in the Senate. [Lane, 2003]

Finally, we find a bill that has had some success. The *Genetic Non-Discrimination Act*, which would (in part) prohibit employers from discriminating against individuals on the basis of genetic information "in any way that would deprive such individuals of employment opportunities or otherwise adversely affect their status as employees." [*Senate*, 2005] This bill has made progress, in twice being unanimously passed by the US

Senate, in 2003 and 2005. However, in neither case has it received a reading in the House of Representatives.

2.4. New South Wales, Australia

Though workplace privacy is not given much explicit legislative protection in North America, prime examples of pro-employee surveillance laws do exist. Perhaps the most comprehensive such law can be found in the Australian state of New South Wales: the *Workplace Surveillance Act 2005*. There are three main aspects to this Act that are applicable to this discussion: mandatory notification of workplace surveillance, a listing of prohibited surveillance, and restrictions on covert surveillance.

Notification

Stringent rules are provided guaranteeing an employee notification of any workplace surveillance. First, any surveillance of an employee is not permitted to commence without prior written notice being provided (notice by e-mail is acceptable as well). Such notice must be provided at least 14 days prior to the commencement of the surveillance, though the employee may agree to a lesser period. This notice must indicate the kind of surveillance (camera, computer or tracking), how it will be carried out, when it will commence, whether it will be continuous or intermittent, and whether it will be ongoing or for a specified period. If camera surveillance is being used, the cameras must be plainly visible, and notices must be posted advising of their presence. Computer surveillance is acceptable only if the employer has provided the employee with a policy document on the matter in such a way that the employee can be expected to be aware of and have understood said policy. Tracking technologies (on vehicles or 'other things') also may not be employed unless a notice is clearly visible on the vehicle or 'other thing', noting that the object is the subject of tracking surveillance.

It is further provided that any surveillance of an employee that does not comply with the appropriate notification policies is considered to be 'covert surveillance'.

Prohibited Surveillance

As well as creating mandatory notification provisions, the *Workplace Surveillance Act* bans some forms of surveillance altogether. For instance, employers are forbidden to carry out any surveillance of change rooms, washrooms or shower facilities. Companies are also not permitted to perform surveillance of employees using 'work surveillance devices' when the employee is not at work, with the exception of allowing computer surveillance of equipment or resources provided to the employee at the expense of the employer. Employers may also not block Internet access or e-mail delivery or reception unless it is in accordance with a distributed policy on the use of these resources, and in the case of blocked e-mails, the employer must provide a 'prevented delivery notice' as soon as is practicable (except in the mail blocked as containing spam, a virus, or as being menacing, harassing or offensive).

Covert Surveillance

Finally, a prohibition of any covert surveillance (that is, any surveillance without notification) is also provided, with exceptions for employers who have applied for (and received) a covert surveillance authority from a Magistrate. Such an authority allows surveillance without notification of any employees while at work, but only for the purpose of establishing whether one or more employees are involved in unlawful activity at work. Such an authority *does not* permit surveillance for the purpose of monitoring an employee's performance. In issuing such an authority, the Magistrate must also consider whether covert surveillance of the employee(s) concerned might unduly intrude on their privacy, or the privacy of any other person. (Exceptions to this rule are also provided in the case of covert surveillance whose purpose is exclusively the protection of employee safety while at work.)

This is what employee privacy legislation *can* be in North America. Rather than a collection of laws scraped together, or vague terms such as 'reasonable person', concrete protections can be provided. At very least, legislation such as this should be debated, if even only to be rejected (as was, for instance, the *Privacy for Consumers and Workers Act* in the US), because such a rejection would serve to clarify the currently rather muddy Canadian legal landscape.

2.5. The Role of Unions

Often overlooked, however, is the role that organized labour can play in the protection of workplace privacy. As of January 1st, 2005, just over 4.38 million Canadian employees (representing 30.7% of Canada's non-agricultural workforce) were unionized; the largest union, the Canadian Union of Public Employees (CUPE), counted some 545,000 members. [Bédard, 2005] This is clearly not an insignificant voice. Should the majority of unions factor workplace privacy protections into collective bargaining agreements (CBAs), a very large effect could be had on what is considered 'reasonable' surveillance. If 30% of the Canadian workforce had their privacy rights protected by union strength, non-unionized employees would have a much greater chance at obtaining the same protections from Canadian law.

Unfortunately, searches of CBAs do not show nearly this kind of movement towards workplace privacy protection. In 1995, a study conducted by Susan Bryant found that though there was 'timid and weak protection from zealous surveillance' in the Canadian constitution, criminal and labour legislation, virtually nothing was being done by trade unions to fill that gap, particularly at the level of collective bargaining. [Bryant, 1995] Nearly a decade later, Kiss and Mosco (2005) performed a search of French and English language collective agreements, with the strings "privacy or monitor or surveillance" and "observational systems" (along with the corresponding French terms). Of the 5,495 agreements searched, only 76 contained language dealing with electronic surveillance in the workplace. The authors do present numerous possible reasons for these results, such as the decline of the industrial economy (which threatens the very existence of many unions), a focus on more 'important' issues (such as job security and wages), and the fact

that historically, electronic surveillance has primarily focused on 'desk' jobs, such as data entry workers or telephone operators – jobs frequently filled by women, whose limited power in unions may make surveillance a difficult issue to promote in the union agenda. [Kiss and Mosco, 2005] The fact remains, however, that less than 2% of collective bargaining agreements in Canada contain any discussion of electronic monitoring or workplace privacy.

Canadian workers, unfortunately, do not fair as well in the absence of any discussion of surveillance within a collective agreement. It has been ruled, for instance, that the absence of any language addressing Internet or e-mail policies in the workplace increases employer rights. Corry and Nutz write, "Even where such rules as an Internet/e-mail policy do not form part of the [collective] agreement, it is now generally conceded … that in the absence of specific language to the contrary in the agreement, the making of such rules or policies lies within the prerogative of management…." [Corry and Nutz, 2003] That is, if a union fails to bargain specific electronic monitoring rights, the company is allowed to do what is necessary to 'manage' the workforce.

This is not to say that unions are necessarily powerless to protect workplace privacy; quite the contrary is true, in fact. Nor, though, can it be said that the mere inclusion of privacy language is a guaranteed protection; in some cases, collective agreements that mention surveillance do so to establish management's right to use it. Kiss and Mosco found that there were four degrees of protection within the 76 collective agreements they examined: low (management rights to monitor explicitly noted; workers are granted only notification), moderate (surveillance practices accepted, but within limits), high (surveillance practices restricted to the narrowest possible category), and worker-friendly (surveillance allowed for protection of employee safety or property). The 76 agreements split into 15 low protection, 32 moderate, 24 high, and 5 worker-friendly. The two extremes, low and high protection, are discussed below.

Low Protection

(All collective bargaining agreement excerpts from [Kiss and Mosco, 2005].)

Low protection collective agreements may be the result of a bargaining decision (i.e. privacy is traded for job security, etc.), or of a low regard for workplace privacy concerns. Regardless, employees subject to such an agreement can expect virtually no privacy protection. For instance, an agreement between Economic Development Edmonton (EDE) and the United Food and Commercial Workers, signed after a drawn-out strike, reads in part: "EDE has the right to manage its business as it sees fit, including the right to utilize any surveillance methods without notice." This is a remarkable *carte blanche*; it is fortunate that these employees are now at least covered by Alberta's PIPA. Less extreme forms of this lack of protection are still troubling, though. An agreement between Loomis Courier Services and the Canadian Auto Workers states: "The following notice will be posted in all work places covered by the Collective Agreement: 'Due to the nature of our business and occasional requests from customers, electronic surveillance equipment may be installed from time to time in the workplace.'" This is less threatening,

but it is still very nearly a case of 'anything goes' surveillance of employees. The United Food and Commercial Workers did slightly better, but not much, with their agreement with Safeway and Overwaitea Foods: "Within the confines of the law, the Employer may use video cameras in almost any part of the store. The vast majority of employees have no need to be concerned and may be assured that common sense and discretion will prevail in choosing who is allowed access to any monitoring equipment or video tapes." There are still absolutely no controls on the uses to which the cameras may be put, though. 'Discretion' can mean that while the average customer may be prevented from viewing videotapes, a manager will review the tapes at the end of each day, and evaluate performance accordingly. This, of course, is not necessarily the situation, but it is also not prohibited by the agreement.

High Protection

In contrast to the above examples, we find that historically strong unions are able to secure their members against virtually all electronic surveillance, at least in as much as preventing employers from using any captured information for disciplinary purposes. The Communications, Energy and Paperworkers union, in an agreement supplementary to an existing CBA, was given a written guarantee that "the Company shall not use video security equipment to monitor employee work performance." Similarly, the very strong, historically-militant Canadian Union of Postal Workers was able to bargain in a CBA clause reading: "The watch and observation systems cannot be used except for the purpose of protecting mail and the property of the State against criminal acts such as theft, depredation and damage to property. At no time may such systems be used as a means to evaluate the performance of employees and to gather evidence in support of disciplinary measures unless such disciplinary measures result from the commission of a criminal act."

Union representatives are very well aware that it is unreasonable to demand that a workplace be completely free of electronic surveillance. These technologies can prove themselves quite valuable to protecting worker safety, or to the prevention of theft of company property. However, a system installed for such a purpose should not be able to gradually become a disciplinary tool, or a productivity monitor. If such a technology is needed, it should be introduced as such; "function creep" of existing systems is what unions are looking to prevent.

The control of electronic surveillance is but a single element of workplace privacy, but strong collective bargaining agreements currently accomplish more towards this end than Canadian privacy law. It is granted that this is partially due to the fact that Canadian law must be appropriate for *all* workplaces, rather than any single workplace as addressed by a CBA, but that is not reason that the 70% of Canadian employees not involved in a union should suffer a greater loss of rights than their organized brethren. CBAs are a prime example of trade-offs between company and employee interests; perhaps future legal discussions of workplace privacy should focus on the compromises made by unions, who have fought to retain the privacy rights of their members.

3. LEGAL PRECEDENT

An examination of Canada's privacy laws is not complete without a similar examination of the ways in which they are currently being applied. Thus, situations in which workplace privacy in Canada has been protected, as well as those situations in which it has been decreased, shall now be discussed. This is not intended as a proper legal review; rather, it is an interpretation of published cases by the a 'reasonable person'. It is important to understand case law through his or her eyes, as it is his or her opinions that must be considered when making rulings based on current Canadian privacy law.

3.1. Closed Circuit Television (CCTV)

By far the most legally challenged privacy-affecting technology in Canada is CCTV. The Privacy Commissioner's Office has seen a broad range of complaints, some well-founded and others not, and when taken as a group, the Office's rulings create a reasonably detailed roadmap of the allowable and disallowed functions of surveillance cameras. Six cases shall be considered here: [*PIPEDA Case Summary 114*, 2003] (and the Federal Court's ruling on this case), [*264*, 2004], [*265*, 2004], [*273,* 2004], [*279*, 2004] and [*290*, 2004].

Issue 1: Cameras used for safety reasons, employees not notified of purpose (Case summary 273)

In 2004, a broadcasting company placed three CCTV cameras on its premises: one outside its building, and two indoors. Employees complained that this was a violation of PIPEDA, as their employer had not made a reasonable effort to disclose the purpose of these cameras. The employer claimed that a memorandum had been posted to such an effect; employees claimed to have no knowledge of this memo.

This was a relatively uncontroversial case for the Commissioner's Office. The company in question was commended for its flexibility and availability, and the case was soon resolved. The Commissioner's Office found that since the cameras were installed for security purposes, and in areas that would only incidentally capture any employee personal information, the company did not need to obtain consent from its employees to install the system. However, the Office did find that principle 4.3.2 of PIPEDA, which requires employers to make a reasonable effort to inform their employees of the purposes of surveillance, had been violated. The broadcaster agreed to develop a policy document regarding the use of the cameras, as well as to tell workers of the intended uses; the matter was thus considered to be resolved.

Issue 2: Cameras used to monitor workstations (Case summaries 279 and 290)

While incidental capture of employee personal data is allowable, focused concentration on their workstations is not. This was made very clear in 2004, when employees of an Internet service provider (ISP) challenged management's installation of two webcams, one pointing towards the sales and marketing staff, and the other towards the technical

staff. The cameras were set to low-resolution, did not record and could not pan nor zoom; however, individuals and their actions could clearly be discerned. Though the cameras were continuously operative, it was claimed that the managers of the two departments would only view the images when they were off-site. The company listed two main reasons for installing the cameras: security and productivity.

Upon consideration of the situation, the Commissioner's Office ruled that neither reason was sufficient for the invasion of privacy created by the cameras. As to the issue of employee performance, the Office noted that there were numerous other productivity measures already in place, including monitored e-mail, automated phone systems, etc. The company contended that it needed the cameras in order to observe and manage employee attitudes and behaviours at times when management was not on location. The Commissioner's Office countered that the ISP had not considered, nor were they willing to consider, alternative solutions such as modifying managerial work hours, or creating supervisory roles for employees. As to the issue of security, the commissioner noted that the company did not provide evidence of problems of theft or harassment, and that less-invasive employee security measures, such as surveillance of entryways, were not being used. Thus, it was considered that a reasonable person would not find that security concerns would justify the use of these cameras.

Finally, the Commissioner's Office commented that it felt that this surveillance was being undertaken solely as a deterrent (to theft, harassment, criticism, etc). It was admitted that privacy-invasive systems tend to fulfill such objectives at minimal financial cost; however, the cost of human dignity must also be considered. The Assistant-Commissioner writes, "continuous, indiscriminate surveillance of employees … [is] based on a lack of trust and treats all individuals with suspicion, when the underlying problems may rest with a few individuals or with a management plan that may not be entirely sound. The effect of such omnipresent observation [is] stifling. … The goal of ensuring adherence to the company's vision comes at too high a price to our individual autonomy and freedom." [*PIPEDA Case Summary #279,* 2004] The ISP was thus ordered to remove the cameras within 45 days.

Approximately six months after issuing this order, a similar case appeared before the Commissioner's Office. In it, a Canadian Food Inspection Agency (CFIA) employee complained that a camera installed in the evisceration room of a meat-packing plant had no purpose but to observe his actions. The company argued that the camera was being used to ensure product safety. The Commissioner's Office rejected this claim, however, noting that the Veterinarian in Charge and CFIA inspectors were present whenever the room was in use, and it was their responsibility to ensure product safety; a camera (which did not provide a clear picture of the animals) was of no assistance to them. There was no purpose for the cameras, it was deemed, other than to scrutinize the CFIA employees; since, it was felt, this would not be considered a reasonable purpose for the invasion of the employees' privacy, the company was ordered to remove the camera.

Issue 3: Cameras installed for other purposes used to confirm suspicion of rule-breaking (Case summary 265)

In February 2004, the Privacy Commissioner's office issued its finding for a case in which an operational camera (that is, a camera used to monitor the day-to-day operations of a company) was used to observe two employees of a railyard leaving the property during working hours. The complainants were spotted entering a vehicle, and their manager used the camera's zoom function to observe them leaving the premises, a violation of company policy. The employees argued that this was an improper collection of their personal information under PIPEDA.

The presence of the camera, in this case, was not at issue, as it had been installed as the result of a risk analysis procedure, and its use was supported by both management and the employees union. Also, it must be noted that PIPEDA allows the collection without consent of personal information when investigating the breech of an agreement. Thus, the Commissioner's Office was asked to rule if such an exception applied in this particular case.

The Office first noted that there was no prior evidence presented that unauthorized absences were a problem for these or any employees, nor that showed any previous, less invasive measures to control such absences. Thus, it was unlikely that a reasonable person would feel that it was acceptable to use a surveillance camera to manage workplace performance issues such as this. Secondly, it was noted that while an organization has the right to initiate an investigation if it has suspicion that a breech of trust has occurred, such suspicion did not exist in this case. The complainants were merely spotted entering a private vehicle; this does not imply any wrongdoing on their part. Thus, such an allowance for collection of information without consent did not apply in this case. It was thus determined that the complaint was *well-founded*, and that the company was not permitted to use the camera in this way.

Issue 4: Cameras installed for other purposes used for disciplinary action, when the information comes in the regular course of business (Case summary 264)

The next case differs in a subtle, yet very important, way from the previous one. In this case, the camera in question monitored the front entranceway to a railyard, storing all information gathered for 30 days. The complainant claimed that he was reprimanded for actions caught by this camera, and that this was an improper use of his personal information. The company contended that the information was gathered during the regular course of business, and that it aided in the investigation of a contravention of the laws of Canada, and thus satisfies the two conditions of use without consent described by PIPEDA paragraph 7(2)(a). Again, the use of the camera for its intended purposes (security) is not in question.

The Privacy Commissioner's Office's investigation found that the video in question showed the complainant on various occasions walking up a ramp that was prohibited to foot traffic for safety reasons; signs stating this rule were posted at the top and bottom of

the ramp. The Canada Labour Code, section 126, states in part that employees must follow proscribed safety procedures while at work; the complainant was not doing so, and thus was in violation of a law of Canada. The question turned, then, to the matter of how the information was brought to the attention of management. As it turned out, the complainant himself had asked that the recorded surveillance video be viewed, in order to support his allegations of harassment by a supervisor. While the tape did not support this claim, it did clearly show the previously described safety violation. Thus, as the complainant's personal information had come to the attention of management during the regular course of business, PIPEDA 7(2)(a) applied. The Commissioner's office ruled that the complaint was *not well-founded*.

Issue 5: Cameras that unintentionally may capture employee work information (Case summary 114)

This incident was the earliest PIPEDA challenge involving workplace surveillance cameras, and has become rather a contentious one. The scenario is simple enough; a railyard installs surveillance cameras to guard against vandalism and theft. Employees are notified of the purpose of the cameras, and told that they will not be used for productivity issues. They are trained at entranceways, and away from work areas; when it is noticed that the cameras may incidentally be capturing work areas, they are re-positioned or fitted with a shield to protect employee privacy. The union, though, objects to the presence of the cameras, arguing that they are not needed.

In deciding this case, the Privacy Commissioner's Office considered a four-point test, which is now frequently used when evaluating surveillance technologies. The points were:

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

The Commissioner's Office argued that there was not actually a demonstrable need for this security measure. If the company could have proven that the cameras were needed to reduce vandalism and improve security, then such a measure would have been acceptable; the Office ruled, though, that no such evidence had been provided. It also found that though no incidents had been reported since the installation of the cameras, warning signs posted on exterior fencing may have been the reason for the reduction. The Office also felt that less invasive measures, such as better parking lot lighting, had not been considered. Finally, it was noted that the mere presence of the cameras may have given rise to the perception among employees that their comings and goings were being monitored (even if that was not objectively the case), and that the adverse psychological effects of a perceived privacy invasion may have been occurring. For these reasons, it was ruled that a reasonable person would not consider such a security measure to be appropriate, and the Office made a recommendation that the company remove the camera.

The recommendation was rejected by the company; thus, as is made necessary by PIPEDA, the employee (Erwin Eastmond) filed a complaint against the company (Canadian Pacific Railway) in Federal Court, asking that this recommendation be enforced. [*Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada,* 2004] The Justice for the case decided that it was his duty to treat this complaint as a fresh application; it was not simply a review of the Privacy Commissioner's report. While some deference would be given to the Commissioner in his area of expertise, it was decided that the evidence presented in this new case was sufficiently different as to warrant no deference being given to the Commissioner's findings of fact.

The Justice began by stating that he was prepared to be guided by the same four evaluatory questions mentioned by the Privacy Commissioner, as described above. He also agreed that constant observation of an employee's working area is offensive in human terms. He writes, "it is difficult to conceive of circumstances in which considerations of efficiency would justify such an affront to human dignity…". He also agreed that surveillance cannot be used without reason, citing a previous arbitration ruling which states: "As a general rule, [the employer's interest] does not justify resort to random videotape surveillance in the form of an electronic web, cast like a net, to see what it might catch. Surveillance is an extraordinary step which can only be resorted to where there is, beforehand, reasonable and probable cause to justify it." However, based on the evidence presented to him, he felt that a reasonable person would consider CP's use of video surveillance appropriate under the circumstances.

First, he notes, the collection is not surreptitious, as warning signs are displayed. The collection is brief, occurring only when an individual is within the camera's field of vision, and it is not limited to employees, as visitors will also be captured on film. Also, the recordings are kept under lock and key, accessible only by managers and CP police, and only when an incident has been reported.

Next, the Justice remarks that he is satisfied that CP has legitimate need for surveillance. CP is allowed, in his opinion, to focus on the future utility of the cameras in deterring theft, vandalism, and protecting employee safety and the security of the hazardous and toxic materials that can be found in the yard.

Finally, the Justice feels that the actual loss of privacy is minimal. Since the recordings are not viewed unless an incident is reported, and the recordings are of areas in which a person has low expectation of privacy (i.e. public places), the Justice finds that the loss of privacy is proportional to the benefit gained. Since the railyard is a large area, as well, alternatives like fencing or extra security staff are not practical; thus, the final part of the Privacy Commissioner's four-part test is also passed, and it can safely be said that a reasonable individual would find this surveillance appropriate under the circumstances.

The final matter that must be addressed is the matter of whether or not CP needed to obtain consent to collect individuals' personal information. The Justice felt that since recordings are not viewed until an incident has been reported, and will otherwise be deleted, it is actually at the time of viewing that collection can be said to have taken

place. Thus, CP's argument that the collection of personal information takes place only during the investigation of an incident, and that such information would not be available if CP had to get an individual's consent to record it (since the individual in question is the perpetrator of the incident being investigated), is valid, and section 7(1)(b) of PIPEDA can be applied, allowing collection without consent.

Thus, the Privacy Commissioner's findings were reversed, and Canadian Pacific is allowed to retain their security cameras.

In general, then, it seems to be the case that so long as employees are informed of the purposes of video surveillance, they are not filmed while actually performing their duties, and the cameras do not develop 'function creep', CCTV installations in the workplace will be allowed. This seems a reasonably fair trade-off between employee and employer interests; so long as further cases bring only clarifications, and not complete overhauls to this system, Canadians should be pleased with the handling of this privacy-threatening technology. However, in other, less examined areas of workplace privacy, there is much work left to be done.

3.2. Mail Opening

On July 15, 2003, the Canadian Privacy Commissioner issued [*PIPEDA Case Summary #190*, 2003], entitled "Bank opens former employee's mail." In this case, a former bank employee complained that his ex-employer had opened mail, both internally- and externally generated, addressed to him, thus improperly accessing his personal information. The bank acknowledged that it had opened the complainant's internal correspondence (a pay statement), but claimed that it did so in order to settle a disagreement over pay initiated by the respondent, and that the manager who opened the mail was authorized to access payroll information. As to the externally-generated correspondence, bank representatives claimed that there was no record of such an incident, but that it was possible that the mail in question was the results of a bank-sponsored course taken by the employee, which the employee necessarily must have authorized his manager to view. The bank indicated that its general practice was to open mail addressed to ex-employees if it appeared to be 'business-related', noting that if a customer were to address correspondence to an individual employee (as frequently occurred), and that employee no longer worked for the bank, it may be a violation of PIPEDA to forward the information (a credit application, or signed document, for instance) to the ex-employee without scrutiny. Bank policy stated that personal mail should not be sent to an individual's work address, as many company units opened incoming mail. Internal mail was to be marked with the term 'Confidential', and would then be delivered unopened to the intended recipient.

As to the first count, of opening internal mail, the bank was found to be in violation of its own policy on opening pay statements, and thus in violation of PIPEDA Principle 4.7, which states that personal information must be protected with adequate safeguards. More interestingly, though, is the fact that the second complaint, that the bank had improperly opened mail from an external source, was ruled to be not well-founded. The

Commissioner stated that not only was the practice of opening mail addressed to an employee reasonable, it could actually be seen to be obligatory.

This decision deserves some reflection, as although it does not constitute legal precedent, it is strongly indicative of the Privacy Commissioner's Office's view on a very important issue. In Canada, outside of a workplace environment opening mail addressed to another person is a felony. Police organizations cannot take such an action without a warrant; in fact, the illegal opening of mail by the RCMP was a large factor in the decision to form CSIS, and take intelligence gathering out of the hands of the RCMP. [Rosen, 2000] Inside the workplace, though, it would seem to be perfectly permissible. In the summary of this case, it was written, "the Commissioner noted that many offices automatically open external mail addressed to employees." This was the entirety of the discussion of this issue. In the opinion of the office dedicated to protecting the privacy of Canadians, the same manager who would be imprisoned for reading his or her neighbour's mail is permitted, if not expected, to read mail addressed to employees in his or her charge.

In a similar vein, employee e-mail is regularly read by employers. Does this case, then, imply that any challenge to such a practice will be dismissed? The fact that many companies have policies allowing them to screen all e-mail should not mean that these rules cannot be challenged.

3.3. Keystroke Monitoring

On June 24, 2005, the Alberta Office of the Information and Privacy Commissioner released Order F2005-003 [*Parkland Regional Library,* 2005], a review of the actions of the Parkland Regional Library. The Library had installed a keystroke logger on the terminal of a computer technician in its employ. The technician found the program approximately a month after it was installed, and deleted it. The information logged was not viewed by anyone but the technician, though Library managers admitted that they did intend to review the data.

The Library defended their actions based mainly on section 33(c) of the Alberta *Freedom of Information and Protection of Privacy Act*, which permits the collection of personal information when it directly relates to and is necessary for an operating program or activity of a public body. The keystroke logger was necessary, it was claimed, in order to effectively manage the technician, and address concerns about his productivity and use of time.

The Information and Privacy Commissioner accepted the argument that if the keystroke logger were necessary to manage the employee, it would be allowed by section 33(c) of the *Act*. Thus, his responsibility was to determine the necessity of such a device. First, he noted that the evidence of improper use of work time by the employee was mostly anecdotal; there was a single instance in which a supervisor noted the technician's personal webpage was displayed on his monitor, and another in which the technician was seen installing a program without prior authorization of his supervisor. There were also issues that had been raised during the technician's probationary interview about his

independent style of work, which was frowned upon by the Library. However, no concrete evidence could be presented to support claims of a lack of productivity.

Upon review of this information, the Commissioner noted that the Library was not justified in the use of the keystroke logger. Such a program, he argued, "involve[s] a continuous monitoring of an employee's working life, [and thus is] highly intrusive into the privacy of employees." The only time monitoring at this level would become "necessary" for a public body's operation, and thus satisfy the conditions of section 33(c) is in the case that there are no other less intrusive means of achieving the desired goal, in this case, of managing an employee. Surreptitious monitoring would only be "necessary" if the information could not be gathered should the employee be forewarned of the monitoring. Since the Library could provide no evidence that simply monitoring the technician's completed tasks would be insufficient to judge his performance, the keystroke logger was not permissible.

However, this is not the end of the story, as further comments by the Commissioner removed the force from this privacy-protecting decision. He notes as an example, "if an employer had reason to believe an employee was using office equipment to surf the net on office time, information collected by keystroke logging software could become 'necessary'." This implies that once an acceptable use policy has been created and distributed to employees, keystroke monitoring is not an extreme measure to ensure compliance. This shows either a lack of understanding of the modern work environment or of the technology in question, or both. Keystroke logging is the single most Draconian computer-based monitoring program currently in use; there are far, far less intrusive measures available to employers wanting to address a relatively minor problem such as improper Internet use. Further, such a logger does not discriminate between work and non-work activity. If, for instance, an employee is permitted to do his or her personal banking using office computers during non-work hours (as was the case at the Parkland Library), any financial information (including account numbers and passwords) would be captured by the logging program. Angry messages written and deleted before being sent, brainstormed ideas, break-time computer usage – all of these actions are captured for the perusal of management. This technology should be reserved for the most extreme of situations, and not deployed simply to monitor Internet usage. The Commissioner may have intended the remark only be an off-hand comment; however, its inclusion in a publicly-available Order brings it dangerously near to the level of precedent.

3.4. Off-Duty Surveillance

In order to examine the Canadian legal precedent for off-duty surveillance, a slight diversion will be taken. Cases of employers being challenged on their monitoring of off-duty activities could not be found; thus, a case of an employer hiring a private investigator to determine the truthfulness of an employee's disability claims will be examined. The basic scenario is shared with standard off-duty surveillance; that is, an employee is recorded while performing activities that have no connection to his or her employment. By examining the steps that must necessarily be shown to have been taken

by the employer prior to hiring an investigator, an attempt will be made to infer a similar burden for all off-duty surveillance.

The incident that will be examined is [*PIPEDA Case Summary #269*, 2004], published in April 2004 by the Privacy Commissioner's Office. The situation was as follows: during the course of his employment, an employee of a company reported a number of work-related injuries. In 2000, he requested that he be re-assigned due to his physical limitations; in 2001, he requested compassionate transfer to another city due to a family member's health. In the meantime, the company offered him a series of temporary positions that were in line with his limitations; each was refused by the employee, who subsequently applied for extended medical leave. Upon being evaluated to be once again fit for work, his absences continued, and he reported further difficulties.

Throughout this process, the company was frustrated in its attempts to obtain up-to-date medical information on the individual. A request for an updated assessment from his physician went unanswered, a rehabilitation program was cancelled due to lack of progress, and an independent assessment was initially refused by the individual. When he finally did agree to this assessment, the examiner ruled that he had both physical and non-physical barriers to returning to work, and that further examinations would likely not reveal his true functional abilities. Later that year, the company hired a private investigator to conduct surveillance on the employee, in order to determine his true functionality. Once it was determined that the individual was misrepresenting his state of health, the company terminated his employment.

In its defense, the company relied on section 7(1)(b) (investigation of a breech of agreement) and 7(2)(d) (use of information collected by 7(1)(b)) of PIPEDA to justify the collection and use of personal information without consent. In examining the case, the Privacy Commissioner's Office noted that for these exceptions to be invoked, there must be substantial evidence that the relationship of trust between employee and employer has been broken, and that less privacy-invasive measures could not be used for the same ends. The Office considered, though, that the employer had for two years attempted to accommodate the individual with his physical limitations, and that these attempts were strongly resisted by the employee. For another nine-month period, the company unsuccessfully attempted to obtain up-to-date medical information; when the employee did agree to an independent evaluation, the company's suspicions were not refuted. Thus, there was sufficient evidence to suspect that the employee was misrepresenting the state of his health. The Commissioner's Office also noted that the company had attempted many less-privacy invasive means of collecting this information, all of which had proven unsuccessful. In light of the fact, then, that this surveillance was undertaken as an absolute final resort, it was deemed to be allowable under PIPEDA section 7(1)(b).

Nearly two years of attempts to collect information about an employee in a non-invasive manner needed to be undertaken before surveillance of his off-duty activities was allowable. While the same standards may not to apply for surveillance of the use of company-provided cell phones or Internet connections, perhaps cases such as this will

limit a company's ability to perform that surveillance at random, in the hopes of uncovering a misdeed.

3.5. Drug Testing

Workplace drug testing is another area that is yet to see a decision by the Privacy Commissioner's Office; however, such rulings can be found within the Canadian court system. Here, two cases will be described: the first, Entrop v. Imperial Oil, was heard by the Ontario Court of Appeal in July of 2000, in regards to a substance abuse policy for safety-sensitive workers in an oil refinery; the second, Milazzo v. Autocar Connaisseur Inc. was heard by the Canadian Human Rights Tribunal, and involves drug testing in the charter bus industry.

Entrop v. Imperial Oil [1995]

Martin Entrop was an employee of Imperial Oil in their Sarnia, Ontario refinery; he had the position of senior control board operator, and was responsible for controlling various oil refinement processes. In 1991, Imperial Oil announced a new drug testing program, which for safety-sensitive positions included random unannounced drug and alcohol testing with automatic dismissal for a positive test (or any other Policy violation), and mandatory disclosure of current or past 'substance abuse problems' with re-assignment to a non-safety-sensitive position upon such disclosure and re-instatement to one's former position only after a 2-year rehabilitation program followed by a 5 year period of abstinence, as well as pre-employment and 'with cause' (i.e. following an accident or other incident) testing for all employees. Upon the institution of this policy, Entrop notified his supervisor that he had previously been an alcoholic, though he had been completely sober since 1984. Due to this disclosure, though, Entrop was removed to a "less-desirable" non-safety-sensitive position (at the same salary level). He filed a complaint about this incident with the Ontario Human Rights Commission, claiming that his right to equal treatment regardless of disability, which drug or alcohol abuse are considered to be, had been violated. Before the complaint could be considered in court, though, Imperial Oil amended its policy, allowing Entrop to return to his position upon accepting a number of post-reinstatement controls, such as random alcohol testing. When an Ontario Labour Board of Inquiry ("the Board") did hear the case, it ruled that Imperial Oil's policy was *prima facie*[1] discriminatory, and not justified as a bona fide occupational requirement (BFOR). The Board awarded Entrop $21,241.93 damages. Imperial Oil, however, appealed this ruling. In July 2000, the Ontario Court of Appeals ("the Court") heard the case.

The Court agreed with the Board of Inquiry that the drug testing policy was *prima facie* discriminatory against drug abusers. Thus, it was left to Imperial Oil to defend its use as

[1] A *prima facie* case is one which covers the allegation made, and which, if believed, is complete and sufficient to justify a verdict in the complainant's favour in the absence of an answer from the respondent.

a BFOR. A 1999 decision of the Canadian Supreme Court found that in order to prove that a *prima facie* discriminatory standard is a BFOR, the employer must establish that:

(i) the standard was adopted for a purpose rationally connected to the performance of the job;

(ii) the standard was adopted in an honest and good faith belief that it was necessary to the fulfillment of that legitimate work-related purpose;

(iii) and that the standard is reasonably necessary to the accomplishment of that legitimate work-related purpose. To do so, it must be shown that it is impossible to accommodate an individual with the same characteristics as the complainant without imposing undue hardship on the employer. [*British Columbia (Public Service Employee Relations Committee) v. B.C.G.S.E.U ("Meiorin")*, 1999]

If this three-step test is met, the standard is a BFOR, and is this allowable under the law.

In the Entrop case, the Court ruled that the first two steps were clearly met: the purpose of the policy (to minimize the risk of impaired performance, and to promote a safe, healthy work environment) is by common sense connected with the performance of this (or virtually any) job, and Imperial Oil went undertook a wide and thorough consultation process before implementing the policy, facts that satisfy the first and second requirement, respectively. Thus, it was left to decide whether the third requirement was also met. This was done on an item-by-item basis.

First, it was determined that drug testing showed neither proof of impairment on the job, nor of a likelihood of future such impairment. The penalty, automatic dismissal, was also determined to be too great for a single positive test, particularly given the fact that such a test does not show current impairment. Pre-employment drug testing suffers from the same two flaws. Imperial Oil's argument that they are entitled to a 'no presence' of drugs or their metabolites standard (as opposed to the standard of 'no impairment') was also rejected as being too arbitrary, given that such presence does not necessarily indicate an inability to perform work safely. Thus, drug testing is not a BFOR. Testing for alcohol, however, is a different matter. The judge in the case was satisfied that a positive breathalyzer test does indicate current impairment, and thus is a BFOR, so long as the sanction for an employee who tests positive is tailored to individual circumstance (automatic dismissal is not acceptable, though). Testing of employees post-incident was also ruled to be permissible, so long as such a test was only a single facet of a larger assessment of drug abuse.

The provisions for mandatory disclosure of current and past substance abuse problems, reassignment and reinstatement were next considered. The Court ruled that these also failed the third test of a BFOR, that of reasonable necessity, for four reasons. Mandatory disclosure of abuse, no matter how far in the past, is not necessary due to the fact the after five years, an individual's probability of relapse is equal to the probability of occurrence in the general public. Should this fact have been taken into account, however, the disclosure policy would have been acceptable. Second, mandatory reassignment is not necessary, as it fails to accommodate individual differences (such as length of time such abuse has been under control). The requirement of 2 years rehabilitation followed by 5

years abstinence before reinstatement also fails to take into account differing recovery rates. Finally, requirements of all reinstated employees to, for instance, indefinitely attend self-help groups or report to a supervisor incidents which make reoccurrence of the problem more likely are too broad, and should not be necessarily applied in all cases. Due to this general failure to accommodate individual differences, these provisions are not BFORs.

Thus, Imperial Oil's appeal was dismissed, and their drug testing policies were ruled to be discriminatory (excepting their policy on alcohol testing, which was deemed to be allowable).

Milazzo v. Autocar Connaisseur Inc. [2003]

As the proceedings of this case are substantially similar to the previous, many details will be omitted. However, the case remains important as a simple change of work environment in this instance changes the essential decision on workplace drug testing.

In *Milazzo*, a driver for motor coach company Autocar Connaisseur, based in Quebec, brought a complaint to the Canadian Human Rights Tribunal after being fired for testing positive for marijuana metabolites. He alleged, as in *Entrop*, that this action violated his rights to equal treatment as a disabled individual. The Tribunal dismissed this charge, finding that Milazzo was a casual user of marijuana, and thus used the drug by choice rather than being addicted (and was thus not disabled). However, a second part of Milazzo's complaint, that the rule itself was discriminatory, was examined in further detail.

In this case also, the Tribunal ruled that Autocar's policy (automatic termination for those testing positive for drugs, their metabolites or alcohol; rehabilitation leave for those who voluntarily admit to drug or alcohol abuse) was *prima facie* discriminatory, and thus had to pass the three-part test of the BFOR to be allowable. Again, the first two parts were passed without argument, leaving the court to rule on the necessity of the rule to accomplish the purpose of promoting road safety. It was at this point that the Tribunal differed from the Court in *Entrop*, as the Tribunal found that random drug testing was necessary to achieve the company's purpose. It ruled that while a positive test does not necessarily imply that a driver was impaired while working, it does raise 'red flags' that that individual is more likely to work while impaired at some point in the future. The Tribunal also found that random drug and alcohol testing served to deter casual users from working while impaired, thus promoting safe driving in at least that group. Also, since the drivers were not generally in a centralized location, it was found that supervisory programs would likely be ineffective in controlling drug abuse. Thus, except for the lack of accommodation for individuals testing positive (it was ruled that they should have the same opportunity to rehabilitate themselves as those who voluntarily admit to abuse), the policy was ruled to be a BFOR, and thus acceptable.

Two cases, two workplaces, and two different rulings on the acceptability of workplace drug and alcohol testing. While it is absolutely certain that individuals who do test

positive for drug use or alcohol cannot be automatically dismissed, and that a test for *current* impairment would be acceptable for those in safety-critical positions, little else can be deciphered. Workplace drug testing, has been ruled both unacceptable, as it fails to test for current impairment, or acceptable, as it serves as a deterrent and can determine if an individual is more likely to work while impaired. Interestingly, though, no challenges are made to drug and alcohol testing on a privacy level; the decisions that exist all challenge the practice as being discriminatory. This is an issue that should be addressed; workplace drug tests are not only discriminatory, but invasive. Perhaps it speaks to the state of current privacy law that no such challenges have been made.

3.6. Other Issues

Certainly other issues do exist; for reasons of space, not everything can be included here. In general, rulings by the Privacy Commissioner's Office tend to prohibit the most blatant of offences (unnecessary collection and mishandling of medical records [*PIPEDA Case Summary 226*, 2003], surreptitious electronic surveillance [*268*, 2004]), while allowing businesses to gather information necessary for day-to-day functionality (such as performance statistics [*153*, 2003]). With the exception of the appeals to these rulings, or decisions made by labour arbitrators, though, workplace privacy is not particularly well examined in Canada. There is very little case law, for instance, governing workplace interception of e-mail. Such an interception, however, is an issue that has been examined at length in the American legal system. As Canadian privacy laws frequently depend on the theoretical opinion of the 'reasonable person', it is worth examining the practices that Americans consider acceptable, as such opinions may easily migrate northward.

3.7. E-Mail Privacy in the American Workplace

Workplace privacy in the United States is given virtually no protection; in fact, work has been done to substantiate the general thesis that "modern [American] workplace workers have almost no rights … civil liberties are shed as the worker enters the workplace." [Rosenberg, 2005] An examination of employees' e-mail privacy rights typifies this assertion. Four cases, from 1992 to 1999, have served to form a precedent that asserts an employee has no control over the use of his or her communications, and that companies have the right to not only generate e-mail acceptable use policies of any form, but also to violate these policies without consequence. These cases, as summarized in [Rosenberg, 2005], are presented below.

Bonita P. Bourke et al. v. Nissan Motor Company [1993]

This case, which was heard in July 1993 by the California Court of Appeal, is important in that it occurred early on during the use of workplace e-mail. In it, the Court of Appeal upheld an original ruling for the defendant, against charges alleging "wrongful termination, invasion of privacy and the violation of [the plaintiffs'] constitutional right to privacy in connection with Nissan's retrieval, printing and reading of e-mail messages authored by the plaintiffs." The charges stemmed from an incident in which a highly personal e-mail authored by Bourke was unfortunately chosen as an example during a

training session. The message was reported to management, who subsequently found other personal messages that had been sent between Bourke and her co-plaintiff, Hall. After receiving multiple low performance evaluations, the two filed a grievance with the company's human resources department. The two then sued Nissan for "common law invasion of privacy, violation of their constitutional right to privacy, and violation of the criminal wiretapping and eavesdropping statutes." The trial court found for Nissan on two grounds, one of which is important for this discussion: "Based on the undisputed facts, plaintiffs had no reasonable expectation of privacy in their e-mail messages." Nissan presented the now-standard argument that if warnings of lack of privacy are made generally known, and that it is made clear that e-mail systems are only to be used for company business, employees have nothing to complain about if their personal messages are discovered.

Alana Shoars v. Epson America, Inc. [1994]

This case, again from the California Court of Appeals, speaks to company management's ability to set rules as they see fit. The plaintiff, Shoars, had allegedly been told in her role as instructor in the use of the company's e-mail system that Epson employees' mail was considered to be private and confidential. However, beginning in 1989, Shoars' supervisor, acting under the direction of the company, tapped into the e-mail system, and began to print out and read e-mail being sent from employee computers. Shoars maintained that she was then fired for her refusal to go along with this interception, which, she claimed, violated Epson's public policy. The Court of Appeals, though, upheld the original trial court's ruling for Epson. Management's control of the workplace became stronger.

Bill McLaren, Jr. v. Microsoft Corporation [1999]

This control was finalized, however, in a 1999 Texas Court of Appeals ruling. The situation, in brief, was that in December 1996, McLaren, a Microsoft employee, was suspended pending an investigation into accusations of sexual harassment. McLaren requested access to his e-mails, in order to disprove the allegations against him; he was told that such access would be granted only if he informed company officials of the location of a particular message. He then requested by memorandum that no-one tamper with his workstation or e-mail; however, his employment was terminated on December 11, 1996.

McLaren's suit against Microsoft involved an invasion claim, alleging that the company 'broke into' his computer. Microsoft's argument, though, was that "[t]he common law of Texas does not recognize any right of privacy in the contents of electronic mail systems and storage that are provided to employees by the employer as part of the employment relationship." McLaren's case was dismissed, and further confirmed that the control of the workplace by management outweighs any claim for individual privacy.

Michael A. Smyth v. Pillsbury [1996]

The previous cases have shown that employers have no need to make any concessions to employee privacy; in *Smyth v. Pillsbury*, it is found that even when such concessions are made, they do not need to be respected. In this case, Michael A. Smyth sued Pillsbury for wrongful termination, which had been based on information obtained from Smyth's supposedly private e-mail. Pillsbury, Smyth claimed, had "repeatedly assured its employees … that all e-mail communications would remain confidential and privileged. [The company] furthered assured its employees … that e-mail communications could not be intercepted and used by [the company] against its employees as grounds for termination and reprimand." The judge in the case, though, found for the defendant, for reasons that are very revealing. The final paragraph of his decision, for instance, reads:

> In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreocer, the 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.

The judge did not accept that the employee in this situation had a reasonable expectation of privacy, due the nature of the comments being transmitted (testified by Pillsbury to include threats). The court declared that once such material had been transmitted to another person, via a system utilized by the entire company, the sender lost any reasonable expectation of privacy.

Thus, regardless of any assurances from a company of the privacy of e-mail, an employee has either no expectation of privacy in his communications, or no claim that invasions of this privacy by his or her employer are substantial or highly offensive. Such guarantees, then, offer no protections whatsoever, and might as well not be made.

Canadians should take note of these rulings. In a span of four cases over seven years, e-mail privacy rights in the American workplace have been decimated. After his review of these cases, Rosenberg [2005] states, "Adherence to basic ethical principles regarding the importance of individual privacy in human affairs has been abandoned at the entrance to the workplace." It is difficult to argue with this statement. Employers are permitted to, for any reason, intercept and read employee e-mail, regardless of any policy that assures employees that this will not be done. In the eyes of American law, a company that breaches its own e-mail policy in order to catch an employee who breaches the same policy is justified in its actions. In matters of electronic communications, at least, employer interests are placed above the interests of ethics. Should Canada decide to

choose the same balance, so be it. However, employees should force such a choice to be made; Canada cannot be allowed to stumble into such a situation by default – an outcome that becomes more likely as years pass, and explicit policies are not generated.

4. THE PROBLEMS THAT REMAIN (AND POTENTIAL SOLUTIONS)

Thus far, this report has been concerned with painting a picture of the Canadian workplace privacy landscape; it must now identify the remaining holes and blemishes, and suggest the ways that they can be corrected. While it is true that the majority of these suggestions will involve strengthening employee rights, the implication should not be that the employer is forgotten. However, it must be recognized that in the absence of explicit workplace privacy protection, the rights of the employee are threatened to a far greater extent than those of the employer. The most that an employer can expect to gain from any legislation is a confirmation of the legality of procedures already available to him or her, whereas an employee may be able to reclaim a lost measure of humanity. It is the employees who need a voice – but it must be remembered that the best way to have that voice heard is not to cry out, but to reason.

4.1. The Adversarial Relationship

The first problem that must be addressed when discussing workplace privacy is the assumption of an adversarial relationship between a company and its employees. It frequently seems that discussions of privacy centre around an employer which believes that its workers would accomplish nothing if it weren't for workplace monitoring, and a workforce who believe that management only watches them in order to identify and eliminate any weak links. Granted, at any particular moment, either of these opinions may be correct. However, when bargaining is done with the assumption of bad faith on the part of the other side, compromises become difficult to reach. Consider, then, if this were not the case (as many management experts suggest *should* be the situation); would open and good faith communication between an employee who asks only for fair treatment, and an employer which asks only for fair output, not solve many workplace privacy issues? Employees may be able to provide the best solutions about how their performance can be measured without invasion of privacy; after all, workers would like to take credit for positive actions, rather than simply take blame for negative ones. An employee who is allowed to examine the evaluation process itself may also be able to identify flaws in his or her own work processes, and thus increase his or her productivity. Further, the employer is the party best suited to be the source of information about employee surveillance. He or she can explain the processes by which any particular method or technology was chosen, the goals that management hopes to accomplish with it, and the benefits of the system to both company and employee. However, in order to explain this information, the employer must have made these evaluations sometime prior; an employee who feels that his or her rights have been violated will not be satisfied with stock answers or empty statements. By ensuring that surveillance systems can be justified to those individuals subject to them, it is may be possible guarantee that unnecessary monitoring does not take place. Statistics confirm [Maltby, 1999] that employees who are treated with trust and respect respond with greater loyalty and productivity; what better way to show such trust than by allowing employees the greatest level of freedom possible in their work environment.

The practical advice to employers: even in the absence of legislation, evaluate the necessity of monitoring programs, and remove any that cannot be sufficiently justified. Then, explain the purpose, use, and necessity of each program to employees; in short, treat your workforce as adults. Similar advice is given to employees: if a monitoring program is offensive, explain why, or how the same goal can be accomplished in a less invasive way. Or, simply explain that a particular form of surveillance makes you uncomfortable, and ask management to convince you it is both non-threatening and necessary. Treat management as if they care about your welfare: in the best case, this will be true. Again, workplace privacy is not inherently adversarial, although it may seem this way. Both sides can come out ahead – and openness is an important first step towards achieving this result.

4.2. PIPEDA's 'Reasonable Person'

To base privacy legislation on the opinion of the 'reasonable person' is perfectly understandable. Such a clause exists in order to allow flexibility in the law, and in order for it to be able to easily adapt to the changes in society. It also allows the law to be technology-independent; an important trait given that the pace of technological innovation far outstrips that of legal reaction. Thus, the 'reasonable person' is an effective acid test when a situation is well established, and the changes being considered are simply technological advances.

The Canadian workplace privacy situation, however, is not necessarily fixed. PIPEDA was meant to serve as the benchmark for privacy protections; thus, it should not have been passive. By the time that Act was introduced, the 'reasonable person' was accustomed to a situation in which workers had few rights. Surveillance cameras were routinely being installed, incoming mail (physical and electronic) was being read by employers as a matter of course, extensive background checks were being performed on every applicant for many jobs: workplace privacy was in a shambles. In this situation, it can only be expected that the 'reasonable person' will believe that each of these measures is 'appropriate under the circumstances'; why else would they be so widespread?

This situation will not change anytime soon. A person need not even look to the United States for an example of rampant workplace privacy violations. In seven of the ten Canadian provinces (and all three territories), protection of private sector employee rights is next to nil. Rosenberg [2005], for instance, discusses the fact that there are hundreds of workers at a McDonald's restaurant in Winnipeg who currently begin and end their shift by placing a hand on a scanner, which then records the employee's identity and the exact moment that he or she clocked in and out. There is no privacy law that applies to these workers. Now, while this may seem like an innocuous use of technology, it remains an uncontested (and uncontestable) introduction of biometrics into a non-safety critical workplace. Should such introductions spread throughout the retail sector, can a 'reasonable person' be expected to reject a spread into public sector (and thus PIPEDA-protected) positions? The answer seems to be a resounding, and disturbing, 'no'.

In a different circumstance, PIPEDA's 'reasonable person' would protect the privacy of Canadian workers. However, as the situation currently stands, this is not the case. The advice that will be provided here is that if legislators are truly interested in protecting workplace privacy, New South Wales-style pro-active legislation should be introduced. That would allow for a stabilization to occur in the realm of employee rights, after which a 'reasonable person' standard could be used. Alternatively, employee privacy, or more privacy in general, should be added as a 'right', such as is this situation in Quebec, or in the eyes of the United Nations. By doing this, PIPEDA would serve only to clarify matters of privacy, rather than to establish them, as it currently does. Appeals to a Charter right seem far more protective than the theoretical opinions of the 'reasonable person.'

4.3. Powers of the Privacy Commissioner

A second, less vital flaw of PIPEDA is in the limitations on the powers of the Privacy Commissioner of Canada. This is not because the Commissioner is not permitted remedial powers; it is entirely justified that matters of enforcement and the award of damages be settled in a proper court of law. Rather, PIPEDA finds its flaw in prohibiting the Privacy Commissioner from reveal the identity of any organization that has had a complaint brought against it. By doing so, companies are given too much leniency to violate privacy laws, knowing that so long as they agree to stop these violations upon an order from the Commissioner, their identities will stay safe (unless an individual attempts to collect monetary damages in Federal Court). While the Commissioner may not be entitled to punish offending organizations, there seems little reason why the public should be prevented from doing so. The invaluable resource that is the 'free market' should be given a chance to penalize those who violate the trust of individuals; this, it would seem, could act as a strong measure of deterrence for companies. It could also be used positively by companies with clean privacy records, which could market themselves as such in the wake of privacy violations by competitors. However, everything hinges upon the public being able to determine the identity of the offender. The solution in this situation: simply remove this restriction from the Commissioner's Office. Allow the violators of privacy rights to be named, and give the free market a chance to assert its power.

4.4. Lack of Anticipation

The problems within the workplace privacy landscape do not lie solely with legislation, of course. Discouraging trends can be identified which seem to pervade all the contributors to the employee rights discussion. One such trend is a lack of anticipation of new technologies, and the privacy problems that they will pose. For instance, Richard Rosenberg, president of the British Columbia Freedom of Information and Privacy Association and member of the board of directors for the British Columbia Civil Liberties Association, says that both of those organizations have recognized a distinct tendency towards reactivity, rather than proactivity, when it comes to evaluating technology's effect on human rights. The groups are currently preparing to form a joint task force dedicated to anticipating technological advancements and their impact on civil liberties.

This lack of anticipation can also be seen in the recent surge of interest regarding RFID tags. It is only now, when these tags have advanced to the point of potential ubiquity, that they are receiving media and legislative attention. These tags have been used to control workplace access for over a decade, though. [Balkovich et al., 2005] Nearly 40 million people in the United States alone carry these chips as access fobs, quick payment cards, or in other forms. [Garfinkel, 2000] Once a technology has reached this level of penetration, it is difficult, if not impossible, to control its impact on privacy (particularly if we rely on the 'reasonable person'). If privacy, and particularly workplace privacy, is truly to be protected, proactive steps must be taken to anticipate future scenarios and propose model controls before the situation occurs.

In support of advice this matter, a study [Balkovich et al., 2005] will be examined. Undertaken in 2005 by the RAND Corporation and entitled "9 to 5: Do You Know If Your Boss Knows Where You Are?", this study aimed to determine whether the workplace privacy impact of future RFID usage could be gauged by inspecting current policies regarding its use. To do this, representatives from six organizations were interviewed regarding their collection, retention and use of records collected through RFID access systems in place. Common features among organizations were then noted. RAND found, for instance, that each of the 6 companies used the records collected for more than just access control; that access control systems were linked with other databases; and that security and employment practices trump privacy concerns (for instance, no company informed employees that access control data was used for other purposes). [Balkovich et al., 2005] These results, while possibly not shocking, do have large implications for the future – for while door access may not be particularly privacy-sensitive, the fact that the records were treated in such a cavalier manner does not bode well for instances in which RFID does generate privacy-sensitive information.

The RAND study is a prime example of the anticipation of future threats to privacy. Similar studies are needed, though, to understand the potential privacy threats associate with undetectable monitoring (even now, Internet and e-mail monitoring programs can be installed remotely, periodically change name and hard drive location, and hide from lists of active programs, all in an effort to avoid employee detection), and the changing nature of the workplace (decentralized, always-connected employees blur the line between on- and off-duty). These issues in particular should be addressed immediately, as in each case, once the associated privacy rights have been breached, they will not be repaired.

4.5. A Lack of Study of the Canadian Workplace

The final issue that will be mentioned is one that the reader may have noticed throughout this paper. It is the fact that by and large, Canadian workplace privacy remains unstudied. When writing on the topic, it is very difficult to avoid heavily featuring American examples, as they are simply what are made available. There is no Canadian equivalent to the American Management Association's annual surveys, there are few well-established legal precedents, and there are limited texts speaking to workplace privacy from a uniquely Canadian perspective (other than analyses of the effects of

privacy laws). Individuals are left to assume that the Canadian workplace is substantially similar to its American counterpart; this, however, may not be true. Some effort is being made in Canada to regulate workplace privacy – it is yet to be seen or measured whether this has made any difference. PIPEDA may be having a significant effect on the workplace, or it may be having none – this is an important fact that must be studied. The lack of concrete knowledge about the state of Canadian workplace privacy is a hole that should be filled. Should this study be extended, consultations will be made with management, law, and organized labour groups, in an effort to determine how *Canadian* workers and employers approach privacy issues, and what policy changes (if any) they feel are necessary in order to protect privacy in the workplace, while still allowing for the effective management of employees. The imbalance of power in the work environment means that employee rights will not necessarily be protected by default; Canada cannot be afraid to develop strong, unique policies in order to create equitable conditions for both employees and employers, and such policies can only arise from a thorough investigation of the Canadian workplace.

5. CONCLUSIONS

> "Continuous, indiscriminate surveillance of employees … [is] based on a lack of trust and treats all individuals with suspicion, when the underlying problems may rest with a few individuals or with a management plan that may not be entirely sound. The effect of such omnipresent observation [is] stifling. … The goal of ensuring adherence to the company's vision comes at too high a price to our individual autonomy and freedom."
>
> - Heather Black, Assistant Canadian Privacy Commission, 2004

> "With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for 'corrective' measures."
>
> - Bruce Phillips, (then) Canada Privacy Commissioner, 1993

The above statements, published over a decade apart, speak to the heart of workplace privacy issues. Employees are not looking gain an advantage over their employers with their challenges to workplace monitoring; rather, workers simply do not want to surrender their humanity in exchange for a job. Unfortunately, if privacy protections are not put into place, this is a trade that many will be forced to make. The legal environment currently favours the employer, as does the general balance of power within the workplace. People are more and more expected to do one of two things: work a mindless, de-humanizing position, or else define themselves by their job. Individuals in the former group are subject to continuous surveillance within the workplace in order to ensure that they do not deviate from the exacting specifications of their tasks, while their personal lives are thoroughly scrutinized to guarantee fitness for duty. Employees in the latter category are given more freedom to complete tasks as they best see fit, but are subject to intense monitoring to make sure that they not misusing time. They are also frequently expected to blur the line between on- and off-duty, as company resources are provided to allow for constant management or client accessibility. These are situations that should not be allowed to continue.

A lack of workplace privacy creates a workforce of automatons – and Canadian law does not do enough to address this. Admirable efforts have been made, but they do not address the many rapidly approaching issues created by the modern workplace. Rules that effectively address an employer's right to monitor computer activity are based on the assumption that that computer is within the workplace; what happens when, as more and more frequently is occurring, that computer moves into the employee's home? What will employers be allowed to do when a simple medical test gives them access to a complete genetic profile? How can an individual complain about workplace monitoring when he or she cannot detect it, or when it is so commonplace that it is deemed 'reasonable'? These are but a few of the questions raised by this report, the answers to which will be vitally important in determining the extent to which Canadian law recognizes workplace privacy, and the legal weight given to this right.

This report has presented a case for the importance of workplace privacy, described the legal climate surrounding this issue, and identified some of the main problems that must be addressed. It is now up to employees, employers and policy-makers to examine these results, challenging or expanding them where necessary, and make any changes needed in

order to create a productive and humane working environment. Strong workplace privacy protection can be beneficial for all parties – labour, management and legal groups must now combine to make it so.

6. References

2005 Electronic Monitoring & Surveillance Survey, (2005, May 18). American Management Association and The ePolicy Institute. Available: http://www.amanet.org/press/amanews.ems05.htm (Last Accessed April 6, 2006).

Alana Shoars v. Epson America, Inc. 1994. No. B073234. In the Court of Appeal of the State of California, Second Appellate District, Division Two, April 14. Available: http://www.law.seattleu.edu/fachome/chonm/CASES/shoars.html (Last Accessed: April 6, 2006).

AMA 2004 Workplace Testing Survey: Medical Testing, (2004) American Management Association. Available: http://www.amanet.org/research/pdfs/Medical_testing_04.pdf (Last Accessed: April 6, 2006).

Armour, S and Appleby, J. (2005, June 13) "Off-duty behavior can affect job" (*USA TODAY*). Available: http://www.usatoday.com/money/jobcenter/2005-06-12-off-duty-usat_x.htm (Last Accessed: April 6, 2006).

Balkovich, E., Bikson, T, and Bitko, G. (2005) *9 to 5: Do You Know If Your Boss Knows Where You Are?* RAND Corporation. Available: http://rand.org/pubs/technical_reports/2005/RAND_TR197.pdf (Last Accessed: April 6, 2006).

Bédard, M. (2005, December 15) "Union Membership in Canada-January 1, 2005", *Human Resources and Skills Development Canada.* Available: http://www.hrsdc.gc.ca/en/lp/wid/union_membership.shtml (Last Accessed: April 6, 2006).

Beer Choice Costs Man Job, (2005, February 14). (*Fox News)* Available: http://www.foxnews.com/story/0,2933,147580,00.html (Last Accessed: April 6, 2006).

Big Brother Nixes Happy Hour (2005, July 27). Eye on the NLRB: Workers Rights Watch. (*American Rights at Work)*, Available: http://www.americanrightsatwork.org/workersrights/eye7_2005.cfm (Last Accessed: April 6, 2006).

Bill McLaren Jr. v. Microsoft Corporation. 1999. No. 05-97-00824-CV. On Appeal from the 116th Judicial District Court, Dallas County, Texas, Trial Court Cause No. 97-00095-F, May 28. Available: http://cyber.law.harvard.edu/privacy/McLaren_v_Microsoft.htm (Last Accessed: April 6, 2006]

Bonita P. Bourke et al. v. Nissan Motor Company (1993). No. B068705. In the Court of Appeal of the State of California, Second Appellate District, Division Five. July 26. Available: http://www.loundy.com/CASES/Bourke_v_Nissan.html (Last Accessed: April 6, 2006).

British Columbia (Public Service Employee Relations Committee) v. B.C.G.S.E.U ("Meiorin") (1999), 176 D.L.R. (4th) 1

Bryant, S. (1995) "Electronic surveillance in the workplace", *Canadian Journal of Communcation,* 20, 505-522.

Corry, D. and Nutz, K. (2003) "Employee e-mail and Internet use: Canadian legal issues", *Journal of Labor Research,* 24(3), 233-256.

Davidson, P. (2006, February 20) "Double-dialers swell cellphone ranks", (*USA Today).* Available: http://www.usatoday.com/tech/news/2006-02-20-two-cellphones_x.htm (Last Accessed: April 6, 2006)

Employed labour force by place of work, by province and territory, (2001 Census). (2004, September 1). Statistics Canada. Available: http://www40.statcan.ca/l01/cst01/labor40a.htm (Last Accessed: April 6, 2006).

Employers Guide to Cell Phone Liability, (2002). Braun Consulting News, 7(1). Available: http://www.braunconsulting.com/bcg/newsletters/summer2002/summer2002.html (Last Accessed: April 6, 2006).

Entrop v. Imperial Oil Ltd. (1995), 23 C.H.R.R. 196 (Ont. Bd.) [2000] O.J. 2689 (Ont. CA). Available: http://www.cdp-hrc.uottawa.ca/hrlc/hrlc2002/entrop.html (Last Accessed: April 6, 2006).

Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada, (2004), FC 852. Available: http://www.lancasterhouse.com/decisions/2004/jun/fcc-eastmond.htm (Last Accessed: April 6, 2006).

EEOC Charge Statistics, FY 1992 through FY 2005 (2006, January 27). U.S. Equal Employment Opportunities Commission. Available: http://www.eeoc.gov/stats/charges.html (Last Accessed: April 6, 2006).

EEOC Litigation Statistics, FY 1992 through FY 2005. (2006a, March 13) U.S. Equal Employment Opportunities Commission. Available: http://www.eeoc.gov/stats/litigation.html (Last Accessed: April 6, 2006).

Fatal occupational injuries by event or exposure, 1999-2004, (2005, August 25). Bureau of Labor Statistics, United States Department of Labor. Available: www.bls.gov/news.release/cfoi.t01.htm (Last Accessed: April 6, 2006).

Garfinkel, S. (2000) *Database Nation: The Death of Privacy in the 21st Century.* O'Reilly Media, Inc.

How Private is My Medical Information, (2006, March). Privacy Rights Clearinghouse. Available: http://www.privacyrights.org/fs/fs8-med.htm (Last Accessed: April 6, 2006).

Internet use hits productivity costs for employers, (2005, June 2). (*PersonnelToday.com*). Available: http://www.personneltoday.com/Articles/2005/06/02/30156/Internet+use+hits+productivity+costs+for+employers+.htm (Last Accessed: April 6, 2006).

Kiss, S. and Mosco, V. (2005) "Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada", *Canadian Journal of Communications,* 30, 549-564.

Lane, F. (2003) *The Naked Employee*, AMACOM.

Libbenga, J. (2006, February 10). "Video surveillance outfit chips workers", (*The Register*). Available: http://www.theregister.co.uk/2006/02/10/employees_chipped/ (Last Accessed: April 6, 2006).

Lockton, V. (2005) *The Technological Assault on Anonymity*. Master's Thesis, Department of Computer Science, University of British Columbia.

Maltby, L. (1999, September). *Drug Testing: A Bad Investment.* American Civil Liberties Union. Available: http://www.aclu.org/FilesPDFs/drugtesting.pdf (Last Accessed: April 6, 2006).

Michael A. Smyth v. The Pillsbury Company. 1996. Civil Action No. 95-5712, United States District Court, E.D. Pennsylvania, January 23. Available: http://cyber.law.harvard.edu/privacy/smyth_v_pillsbury.htm (Last Accessed: April 6, 2006).

Milazzo v. Autocar Connaisseur Inc., (2003). 47, C.H.R.R. D/468, 2003. Available: http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=502$lg=_e&isruling=0 (Last Accessed: April 6, 2006).

Normand, J. (1994) "Under The Influence? Drugs and the American Workforce", National Academy Press.

Occupational Injuries by Accident Type and Occupation in British Columbia, 1997-2004, (no date). "Table 8". WorkSafe BC. Available: http://www.worksafebc.com/publications/reports/statistics_reports/occupational_injuries/1997-2004/assets/pdf/Table%20%2008%2097-04.pdf (Last Accessed: April 6, 2006).

Parkland Regional Library, (2005, June 24). Order F2005-003, Office of the Information and Privacy Commissioner, Alberta. Available: http://www.oipc.ab.ca/ims/client/upload/F2005-003.pdf (Last Accessed: April 6, 2006).

Phillips, B. (1993, June 30) *Privacy Commissioner – Annual Report 1992-93.* Canada Communication Group. Available: http://www.privcom.gc.ca/information/ar/02_04_01a_e.pdf (Last Accessed: April 6, 2006).

PIPEDA Case Summary #114. (2003, January 23). "Employee objects to company's use of digital video surveillance cameras". Available: http:www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #153. (2003, April 14). "Telecommunications company does not improperly collect or use employee statistics". Available: http:www.privcom.gc.ca/cf-dc/2003/cf-dc_030414_3_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #190. (2003, July 15). "Bank opens former employee's mail". Available: http:www.privcom.gc.ca/cf-dc/2003/cf-dc_030715_01_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #226. (2003, October 31). "Company's collection of medical information unnecessary; safeguards are inappropriate". Available: http:www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #264. (2004, February 19). "Video cameras and swipecards in the workplace". Available: http:www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #265. (2004, February 19). "Video cameras in the workplace". Available: http:www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #268. (2004, April 12). "Electronic monitoring does not yield any information, but practice is strongly discouraged". Available: http:www.privcom.gc.ca/cf-dc/2004/cf_dc_040412_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #269. (2004, April 23). "Employer hires private investigator to conduct video surveillance on employee". Available: http:www.privcom.gc.ca/cf-dc/2004/cf-dc_040423_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #273. (2004, May 18). "After installing surveillance cameras in the workplace, a broadcasting company has agreed to inform its employees about the purpose and to adopt a policy regarding its use". Available: http:www.privcom.gc.ca/cf-dc/2004/cf-dc_040518_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #279. (2004, July 26). "Surveillance of employees at work". Available: http:www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp (Last Accessed: April 6, 2006).

PIPEDA Case Summary #290. (2005, January 27). "Video surveillance cameras at food processing plant questioned". Available: http:www.privcom.gc.ca/cf-dc/2005/290_050127_e.asp (Last Accessed: April 6, 2006).

Privacy Legislation in Canada (2004, October). Office of the Privacy Commissioner of Canada. Available: http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp (Last Accessed: April 6, 2006).

Rosen, L. (2004) *The Safe Hiring Manual*, Facts on Demand Press.

Rosen, P. (2000, January 24) *The Canadian Security Intelligence Service.* Parliamentary Information and Research Service. Available: http://www.parl.gc.ca/information/library/PRBpubs/8427-e.htm (Last Accessed: April 6, 2006).

Rosenberg, R. (2005) "The Technological Assault on Ethics in the Modern Workplace", *The Ethics of Human Resources and Industrial Relations, Ed. Budd, J and Scoville, J.* (144-171).

Sarche, J. (2005, May 17) "Man Says He Was Fired for Drinking Coors", (*ABC News*). Available: http://abcnews.go.com/US/wireStory?id=767156 (Last Accessed: April 6, 2006).

Senate Passes Genetic Non-Discrimination Act (2005, February 25). (*Center for Health and Health Care in Schools)*. Available: http://www.healthinschools.org/2005/feb25_alert.asp (Last Accessed: April 6, 2006).

Shoplifters and Dishonest Employees Continue to Steal Profits From United States Retailers, (2005). Hayes International. Available: www.hayesinternational.com/thft_srvys.html (Last Accessed: April 6, 2006).

Smith, R. E. (2000) *Ben Franklin's Web Site 6*, Sheridan Books.

Stop Snooping, (No Date). Hazards Magazine. Available: http://www.hazards.org/privacy/ (Last Accessed: April 6, 2006).

Westin, A. (1970), *Privacy and Freedom*, Atheneum.

Whittier, J. G. (1856) *Maud Muller.*

Work at Home in 2004, (2005, September 22). Bureau of Labor Statistics, United States Department of Labor. Available: http://www.bls.gov/news.release/pdf/homey.pdf (Last Accessed: April 6, 2006).

Wright, T. (1993, November) *Workplace Privacy: The Need for a Safety Net.* Informaiton and Privacy Commissioner/Ontario. Available: http://www.ipc.on.ca/docs/safnet-e.pdf (Last Accessed: April 6, 2006).

Zwirn, E. (2006, February 16). "Security company gets under the skin with embedded access chips" (*Security Systems News)* Available: http://www.verichipcorp.com/news/1140111202 (Last Accessed: April 6, 2006).