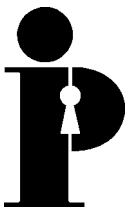
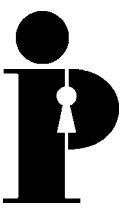
Information
and Privacy
Commissioner/
Ontario

Workplace Privacy:
A Consultation Paper



Tom Wright
Commissioner
June 1992



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Foreword

Over the last decade, public opinion surveys have consistently revealed that a majority of those questioned were concerned with what they perceive to be an erosion of personal privacy. This perception of increasing intrusiveness ranges over nearly all aspects of daily life, from unsolicited telemarketing techniques and inquisitive bureaucrats wanting personal details, to businesses asking for personal identifiers, such as the Social Insurance Number. Every organization, whether public or private, appears to generate an endless demand for personal information.

Privacy is not, however, without its defenders. Supreme Court Justice La Forest has stated:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. … Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated.

Such rules have been adopted by many countries and jurisdictions with the passage of privacy and data protection legislation and the creation of associated commissions.

For those concerned with the protection of personal privacy, the challenge is to explore the implications for privacy of various trends in society, particularly the rapid development of various computer, electronic and scientific technologies. In Ontario, the Information and Privacy Commissioner is charged with researching these issues and raising them for public debate.

This paper deals with what could be termed "workplace privacy." Some people would argue that our expectations of privacy should not be high during the time that we pursue our livelihoods, and that privacy should be subordinate to other values, principally, the collective effort of achieving the goals and objectives of the organization. Privacy, at best, finds an uneasy place in these circumstances. However, privacy advocates would contend that, at a minimum, personal privacy should not be dismissed from serious consideration as a human value that has a legitimate place in the workplace. Some would go even further and argue that protecting the privacy of individuals in the workplace will become one of the leading social issues in the future.

Without some measure of privacy, employees may find themselves without control over their personal information, their behaviour or their person. The potential exists for employers to know about all aspects of their employees' lives including their health, genetic and psychological make-up, finances, schooling, past experience, how they spend their private time, and how they behave in the workplace from minute to minute. In effect, employees may become transparent to their employers.

The arguments in favour of employers needing to collect so much personal information largely turns on the issue of efficiency. Knowing all there is to know about an individual permits monitoring, surveillance, and control, with the ultimate purpose of increasing efficiency and productivity. While these may be worthy goals, should they always be paramount? Can privacy be maintained without sacrificing efficiency? These questions are not easily answered. Perhaps at this point in time, we can do no better than raise the questions.

The aim of this paper is to inform the reader of the various techniques being used in today's work environment and then raise the principal privacy concerns relating to these practices. Finally, we propose various options on how to begin to resolve the issues raised.

Tom Wright
Commissioner

Executive Summary

Although the right to privacy is not explicitly guaranteed in the *Canadian Charter of Rights and Freedoms*, it has been recognized as a fundamental value in a number of recent Supreme Court of Canada decisions. Privacy is difficult to define because its meaning may change from one context to another. Nevertheless, three distinct types of privacy have emerged: territorial privacy, privacy of person, and informational privacy, each of which is relevant to this paper. The convergence of a variety of social, economic and technological trends has placed workplace privacy in jeopardy.

Privacy in the workplace is a relatively new area of inquiry and concern. Today, people are coming to believe that the rights associated with citizenship in society, such as free expression, privacy, equality, and due process, should also be available in the workplace. However, the potential for conflict exists as employees begin to assert their right to privacy at a time when employers are probing more deeply into workers' activities, habits and health than ever before.

To explain why workplace privacy is a growing concern, this paper examines three central issues: the use of electronic monitoring, employee testing, and the misuse of employment records.

Practices and Techniques

The marriage of computers and telecommunications to surveillance practices has quantitatively and qualitatively changed the nature of monitoring in Canadian workplaces. For the purposes of this discussion, electronic monitoring means the collection, storage, analysis, and reporting of data on employee performance and work activity through the use of computer and telecommunications devices (e.g., telephones). Electronic monitoring in the workplace is the daily reality of hundreds of thousands of Canadian workers.

Visual surveillance devices, such as closed circuit television systems, are often considered the most commonly used in the workplace. Telephone surveillance, in the form of call management systems and service observation, is being used to monitor employee telephone activity and to collect performance data. Computer-based monitoring uses specifically designed software to collect performance data for employees working on computers from the time they log on to the time they log off. Access control systems, such as cardkeys and keypads, are also used for surveillance purposes. Some access control devices utilize biometric technology to verify an individual's identity. A final type of monitoring is electronic vehicle tracking which tracks vehicles by using a transmitter or transponder attached to the vehicle.

Advances in technology, medicine and the social sciences have lead to the development of a number of employee testing practices into the workplace. The main testing practices are:

- **Drug testing** to determine if an individual is currently using or has recently used drugs or alcohol.
- **Genetic testing** to detect an individual's genetic predisposition to various conditions.
- **Lie detectors** to measure an individual's physiological responses, in an effort to determine if the individual is telling the truth.
- **Psychological testing** to measure an individual's psychological traits.

Today, employers are relying on these techniques to supplement their knowledge about prospective and current employees.

Employers maintain personnel files and other types of employment records for a wide variety of reasons. Some of this information relates directly to employment decisions (e.g., job applications and performance reviews). However, employment records may also contain sensitive information such as credit ratings, letters of recommendations, and confidential medical information.

New employment practices are being used in the workplace to achieve goals ranging from higher productivity, better employee health and safety, to lower rates of accidents. However, while employers argue that they need to use these practices for valid business reasons, opponents argue that they may destroy the quality of work life.

Privacy Concerns

Privacy advocates maintain that certain employment practices are highly intrusive and a threat to workplace privacy. Their main concerns regarding electronic monitoring, employee testing and the misuse of employment records are as follows:

- **Loss of Personal Autonomy:** There is a concern that intrusive employment practices, such as electronic monitoring, can result in a loss of personal autonomy for the affected workers.
- **Lack of Consent:** Employment practices such as electronic monitoring or employee testing may be introduced without consultation with affected employees. In these instances, workers are not given the opportunity to consent to the practice or to the subsequent collection of their personal information.
- **Invasion of Privacy of Person:** One of the most critical privacy issues relating to both drug and genetic testing is that they are seen as an invasion of the body and a direct violation of the privacy of the person.

- **Invasion of Informational Privacy:** Central to the concept of informational privacy is the ability to determine when, how, and to what extent information about oneself is communicated to others. While this issue is by no means confined to the workplace, some maintain that the loss of control over personal information is perhaps the most significant of all privacy issues.

  The code of fair information practices is an internationally recognized standard regarding the protection of informational privacy. However, intrusive employment practices have the potential to contravene the code. Specific concerns revolve around:

  - the collection of unnecessary and irrelevant personal information;
  - the monitoring of non-work-related activities;
  - the use of inaccurate personal information;
  - the unauthorized use and disclosure of personal information; and
  - the denial of access and right to correct employment records.

- **Expansion of Practices:** The impact of the practices discussed in this paper on individual employees, the workplace in general and on society as a whole, has yet to be fully realized. Many privacy advocates fear that the use of intrusive employment techniques will only increase as new applications are devised and the cost of the technology decreases.

- ***Charter* Issues:** In addition to these specific privacy issues, there is a concern that basic legal principles are being compromised by the use of intrusive techniques in the workplace. Some think that these practices may also raise issues under the *Canadian Charter of Rights and Freedoms* including: presumption of innocence, due process, search and seizure, and equal protection.

Current and Future Considerations

Unchecked technological development is becoming a major threat to personal privacy. Highly sophisticated technology allows for the penetration of physical barriers that, in the past, served to preserve privacy. It also renders traditional legal protections largely inadequate.

Over the past decade or so there has been a growing awareness that workplace privacy issues must be addressed. Some limited measures have already been taken to regulate telephone monitoring, lie detectors, drug testing, and the use of employment records. Newer techniques such as computer monitoring and genetic testing do not yet have any form of government regulation.

The legislative regulation of potentially intrusive employment practices is piecemeal, at best, thereby providing insufficient protection against potential abuses. Although guidelines and court decisions are helping to further define workplace privacy rights, some privacy advocates are concerned that the pace of these developments is too slow.

In unionized workplaces, employment practices may be restricted through collective agreements. Although labour arbitration cases have developed a right to privacy in the workplace, the collective bargaining process is viewed as not being a sufficiently far-reaching and powerful tool to regulate employment practices such as employee testing and electronic surveillance.

The call for legislative action and the cessation of certain practices has been heard for sometime. The most recent call regarding drug testing was the February 1992 submission to the Ontario Minister of Labour by the Canadian Civil Liberties Association (CCLA). The CCLA urged the Minister to introduce legislation that would prohibit employers, on a universal or random basis, from requiring employees or prospective employees to provide urine samples or other bodily fluids for drug testing.

Some observers think that the use of practices such as electronic surveillance in the workplace has already achieved such an inexorable momentum that it may be impossible to stop. They see the real issue as not whether a practice should be used, but rather how its use can be the least damaging for employees. If the status quo is determined to be unsatisfactory, there are a number of different ways in which to proceed.

1. Voluntary Guidelines

The development of voluntary guidelines could take several forms. The Ontario government could:

- encourage employers to create their own guidelines;
- develop guidelines in concert with labour and employer groups, and then encourage employers to adopt them; and/or
- designate an agency (e.g., the Office of the Information and Privacy Commissioner/Ontario or the Human Rights Commission) to review independently developed guidelines to ensure that they met minimum standards set by the government.

Government initiatives in setting guidelines or minimum standards would help ensure that the needs of all affected parties were addressed and a consensus among the stakeholders reached on a number of issues such as: who would be covered (public or private sector, or both), how the guidelines would be introduced, how they would be enforced, and whether there would be an appeal mechanism.

2. Draft Legislation

Another approach would be to regulate employment practices like employee testing, electronic monitoring, and the misuse of employment records through legislation. As several pieces of legislation already address certain employment practices in Ontario (e.g., the *Employment Standards Act*, the *Labour Relations Act*, and the Ontario *Human Rights Code*), this option may be seen as a logical extension. As the scope of each of these pieces of legislation is different, the advantages and disadvantages of each must be carefully examined in order to determine which statute(s) should be amended.

How legislative regulation is introduced could vary:

- the different practices could be addressed separately under different statutes, or dealt with in a single piece of legislation; or
- existing statute(s) could be amended or new legislation introduced.

Due to the limitations of the existing legislation (e.g., some are only applicable to the public sector, and some do not have regulatory agencies with order-making powers), the most appropriate option may be to draft legislation to specifically address this new generation of employment practices.

3. Further Study

As limited research has been conducted on the extent and impact of these new workplace practices, it may be premature to attempt any form of regulation at this time. Accordingly, further study of these issues in the form of a government initiative with consultation with business, labour and advocacy groups, is another option. After such a study, the government would be in an excellent position to determine what, if any, regulatory scheme would be most appropriate.

Table of Contents

Introduction

The Supreme Court of Canada has recognized privacy as a fundamental value in Canadian society:

> … society has come to realize that privacy is at the heart of liberty in a modern state … Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual.[1]

Although the right to privacy is not explicitly guaranteed in the *Canadian Charter of Rights and Freedoms*, it is seen as an essential component of individual dignity and autonomy.[2] The term privacy was defined in the ground-breaking Brandeis and Warren article of 1890 as "the right to be let alone."[3] It has also been identified as a protection against unwanted imposition or coercion by others and a protection of one's freedom of action.[4] "The freedom involved in privacy is not a freedom to act, but a freedom to prevent others from acting, a freedom to exclude."[5]

Privacy is difficult to define because it is a term used to describe a variety of related states of affairs or conditions, the meaning of which may alter from one context to another.[6] Nevertheless, three distinct types of privacy have emerged:

- **Territorial privacy** establishes a physical domain within which a claim to be left alone and a right to repel intrusion is advanced and recognized.
- **Privacy of person** derives from laws that guarantee freedom of movement and expression, prohibit physical assault, and restrict unwarranted search or seizure of the person. While privacy of person encompasses the notion that the person is protected against physical harassment, it transcends the physical and is aimed at protecting the dignity of the person as well.
- **Informational privacy** is based on the notion that all information about an individual is in a fundamental way his or her own, to be communicated or not as the individual determines.[7]

The idea that an employee has a right to privacy within the workplace, either to be free from intrusion or to keep certain information private, is relatively new. Until the 1950s, the right of employers to inquire into any aspect of an employee's life was virtually undisputed.[8] However, today people are coming to believe that the rights attached to citizenship in society, such as free expression, privacy, equality and due process, ought to be available in the workplace.[9] Employees are beginning to assert their right to privacy at a time when employers are probing more deeply into workers' activities, habits and health than ever before.[10]

Privacy is not an absolute. To determine the place of privacy in society, competing values must be balanced. It is no different in the workplace. However, the convergence of a variety of social, economic and technological trends has placed privacy in the workplace in jeopardy. New practices are being introduced into the workplace to address problems ranging from low productivity to high

rates of on-the-job accidents and internal theft. These problems are real and costly for both the employer and society. For example, as substance abuse has negative impacts far beyond the office walls, workplace programs that identify persons with alcohol or drug dependencies and offer assistance may be considered desirable for the affected individuals, the employer and society as a whole.

The difficulty with some workplace practices and technologies is that they can be highly intrusive. While employers argue that they need to introduce these practices for valid business reasons, worker and privacy advocates maintain that certain technologies violate human dignity and personal privacy, and contribute to a degradation in the quality of working life.[11]

Some observers believe that technology could even change the very concept of privacy itself. In the name of improving company security and enhancing productivity, intrusions that would have been questioned or rejected in the past are now being accepted. The boundaries between acceptable and unacceptable intrusions are now less clearly drawn than before.[12]

To explain why employers and employees hold opposing views on these issues, this paper examines three issues in the area of workplace privacy: the use of electronic monitoring, employee testing, and the misuse of employment records.

- **Electronic Monitoring:** Electronic monitoring refers to the collection, storage, analysis, and reporting of data on employee performance and work activity through the use of computer and telecommunications devices (e.g., telephones). Visual, telephone and computer monitoring, along with access control systems and electronic vehicle tracking are discussed.

- **Employee Testing:** Advances in technology, medicine and the social sciences have led to the development of many new employee testing practices. This paper addresses drug, genetic, lie detector and psychological testing. (The issue of HIV/AIDS testing has been examined in previous papers by the Office of the Information and Privacy Commissioner/Ontario, and is not included in this paper.)[13]

- **Employment Records:** Employers collect and use large amounts of information about their employees. Much of this information is highly sensitive and personal in nature, but only some of it directly relates to employment decisions. This paper focuses on the misuse of employment records and the associated privacy concerns. As the results of electronic monitoring and employee testing may form part of employment records, the three issues often overlap.

This paper is divided into three parts. The first section describes the technology associated with electronic monitoring and employee testing, the rationale for using these practices, as well as for the creation of employment records. The second part discusses the privacy concerns raised by testing, surveillance and the misuse of employee information. Finally, the existing legal and regulatory framework and possible options for future action are presented.

Part 1 — Practices and Techniques

Employers have always felt it necessary to collect information about their employees. However, technology has greatly enhanced the ability of the employer to gather detailed personal information about both current and prospective employees. Electronic surveillance technology has made it possible for employers to constantly know what their workers are doing and how well they are performing. Technology also allows employers to identify an employee's genetic structure and drug consumption.

This section of the paper provides a description of various methods of electronic monitoring used in the workplace; a summary of testing techniques; an introduction to the type of records maintained by employers; a review of the various justifications used to support the creation of employment records and the introduction of monitoring and testing practices; and a discussion of some of the general concerns about the use of these techniques in the workplace.

A. Electronic Monitoring Practices

Electronic monitoring in the workplace is the daily reality of hundreds of thousands of Canadians.[14] The marriage of computers and telecommunications to surveillance practices has quantitatively and qualitatively changed the nature of monitoring. Workplace monitoring is no longer limited to what supervisors can immediately observe or hear. Nor are employees always able to know when they are under surveillance.[15] Electronic monitoring can provide a continuous minute-by-minute record of employee performance or activities and, in some cases, it can be used to speed up the pace of the work or enforce work standards.[16] New technology used for surveillance purposes also enables an employer to generate information about an employee that even that individual does not possess. In addition, electronic surveillance is increasingly automatic and triggered by the employee. A worker who enters a parking garage, office, or secure floor using a magnetic stripe card can initiate the creation of a record noting the date and time of entry. The act of logging on to a computer may begin the documentation of files entered, keystrokes and errors made, and messages sent and received.[17]

Electronic monitoring is difficult to define precisely as it is not limited to any one particular type of technology. Also, electronic surveillance practices are constantly evolving as technology itself changes. However, for the purposes of this discussion, electronic monitoring means the collection, storage, analysis, and reporting of data on employee performance and work activity through the use of computer and telecommunications devices.

i) Visual Monitoring

Visual surveillance devices are considered to be the most commonly used in the workplace.[18] They range from still and motion cameras, visual "screens" that appear to be opaque walls, to scanners that can read the contents of unopened envelopes and packages.

Generally, closed circuit television systems (CCTV) allow for observation of multiple locations from a single console with a permanent record being made on tape. Some systems enable the user to "zoom" in on individuals or objects for close observation,[19] or to produce accurate images in near total darkness. Certain CCTV systems are designed so the cameras function continuously, while others have cameras that are only activated upon command or that function on a schedule. Depending upon how a system is configured, the individuals under observation may or may not know when a camera is functioning (e.g., a red light often alerts workers that a camera is activated). "Dummy" cameras are sometimes used to give the impression of surveillance when none is occurring. In addition, advances in miniaturization have meant that visual surveillance devices are now compact enough to fit into a pocket or smoke-detector.

In comparison with other electronic surveillance practices, the use of CCTV systems for employee monitoring is relatively long-standing. One of the first experiments in Canada was conducted in a post office in Peterborough, Ontario, in 1956.[20] However, the technology is continuously being refined. In 1990, a Montreal-based firm launched the first remote video surveillance system in Canada to transmit pictures over regular telephone lines. This system can transmit video, audio and data anywhere in the world with a telephone network. It also allows a user to monitor what is going on at a location miles away, whereas traditional video surveillance systems only operate within the site they are installed. The company that developed the system envisages potential use by retail stores, shopping centres, government institutions, police forces, hospitals, and "any organization that wants to keep an eye on things from a distance."[21]

ii) Telephone Monitoring

Telephone call accounting or management systems are designed to automatically generate detailed information on telephone usage including: incoming and outgoing call numbers, total number of calls made, and total time on the line. This raw data is processed by computer to provide reports on any telephone activity the employer thinks relevant or useful. These systems generally do not provide information on the content of telephone calls.[22]

More and more private sector businesses and government institutions are becoming aware of the economic value of accurate records of telephone calls. Accordingly, organizations install call accounting systems to:

- determine cost allocation between different parts of an organization;
- provide a cross-check of the reasonableness of the telephone bill;
- improve system design and management; and
- improve telephone practices.[23]

The information generated can be extremely useful to companies concerned with customer service. Knowing the number of seconds a customer waited before someone was available to assist them, or how many calls were abandoned, assists companies to determine if additional telephone lines or operators are required. Analysis of daily or monthly telephone work volumes can also help managers better understand cycles in their business so they can predict busy periods when they must add lines, hire temporary workers or offer overtime.[24]

However, employers are increasingly using telephone call management systems to monitor employee telephone activity and to collect performance data. This practice is used primarily by firms engaged in telemarketing, direct sales, and market research, and by companies with large customer service departments. One of the foremost examples of telephone call accounting for performance monitoring occurred within a Canadian telephone company. The president of the local union reported that:

> With the touch of a few keys, management is delivered 75 pieces of data on an operator's performance. The manager is aware of the operator's overall performance in terms of average work time per call and what percentage of the time the operator was away from the machine.
>
> If in the opinion of management, the operator is not meeting objectives, [he or she] can be questioned with respect to the average number of seconds required to depress the first key after a customer comes on the line, the average number of letters per entry, the average number of corrections per call, the average number of seconds to key the data, and much more.[25]

Another form of telephone monitoring is service observation which involves listening in on and/or recording calls to determine the content of employee telephone calls. Observation is generally done by a supervisor or quality control officer to evaluate employee courtesy, the accuracy or correctness of information disseminated, compliance with company guidelines, or knowledge of product. This practice is not automated like telephone call management systems. It involves a human listener making judgments on the content of a call.[26]

In the past, lack of sophistication in technology meant that the employee, and possibly the caller, were aware of when service observation took place. With some older telephone systems there was a drop in volume or a click when the observer came on the line. Today, advances in technology allow the equipment to be silent so that neither party on the line is aware of the observation.

With the advent of voice-messaging or voice-mailboxes, a new type of telephone monitoring has developed. Some companies review employee phone-mail greetings to check for appropriateness.[27] There is also the potential to play back messages left to determine if they are work-related or personal.

iii) Computer Monitoring

Computer-based monitoring is one of the fastest growing areas in workplace surveillance. Using specifically designed monitoring software, employers can now collect performance data for employees working on computers from the time they log on to the time they log off.

In the late 1980s, a study of about 1,500 employees in 50 Canadian firms was conducted on computerized performance monitoring and control systems.[28] From this study it was determined that computer monitoring systems are capable of executing a variety of tasks depending upon their design and purpose:

- Some monitoring systems merely collect statistics about performance (e.g., word-processor logs that count lines or keystrokes) and aggregate them into periodic summaries. Other systems evaluate these statistics, while still others actually direct work to employees.
- More sophisticated designs can alert supervisors when a worker is not connected to the system or they may also compare actual performance to productivity standards on a minute-by-minute basis.
- Systems can feed performance data back to the employee to allow self-monitoring or they can send the information directly to supervisors.[29]
- Computer work monitoring can give information on individual performance or provide a picture of the aggregate performance of a work group or department.
- Statistics on patterns of performance can be used to estimate future workloads, to plan for new personnel or to justify new equipment.
- Computer-generated statistics may also be used to measure employee performance and may be tied to personnel decisions such as pay increases, promotion, retraining and discharge.[30]

A new type of computer monitoring involves the use of electronic mail (e-mail) for surveillance purposes. From the moment a sender creates an e-mail message until it is read by the recipient, the material is in an electronic form that may be readily intercepted and read by anyone with the necessary equipment.[31] It may also be read from either the sender's or receiver's mailbox. Employers are now using these vulnerabilities in electronic mail to monitor employee electronic correspondence.

Computer monitoring is not just confined to white-collar workers in offices. Wherever a computer is used, monitoring can occur. For example, a small computer called "Tripmaster" may be mounted on the dashboard of any vehicle to keep track of variables including speed, gear shifting, excessive idling, when and how long the driver stops, and the number of times the rear door of the trailer is opened.[32]

iv) Access Control Systems

Still another form of electronic surveillance may be undertaken through access control systems; cardkeys and keypads being the most common. As this technology has become more sophisticated, its application has expanded beyond just physical access control to data security. Now these systems are considered to be an important part of any security plan because they can:

- control access to the physical environment;
- limit system user access to information and systems resources;
- monitor system user activity;
- report on security violations for follow-up; and
- monitor employee attendance.

Often issued to an employee for company security purposes, these cards or keys also enable the employer to track employee movements. Depending upon how a system is configured, an employer may be able to know exactly where each staff member is and for how long, including the washroom, lunchroom, computer facility, and parking lot.[33]

Some access control devices utilize biometric technology to verify an individual's identity. Five biometric technologies are currently on the market: fingerprint patterns, hand geometry, retinal scanner, voice verification, and signature dynamics. The shape of a hand, the vein pattern in an eyeball, and the line pattern in a fingerprint are inborn traits, while the pressure points of a signature and the acoustic variations in a voice pattern are behavioral traits. Biometric access control systems are widely considered to be the ideal method for securing physical sites or information systems. However, biometric system are generally used in conjunction with some other means of identifying an individual, such as a personal identification number.[34]

v) Electronic Vehicle Tracking

Electronic vehicle tracking is yet another type of electronic monitoring. The position of a vehicle may be located and tracked by a transmitter or transponder attached to the vehicle. This technique is used by employers to monitor the movements of employees driving vehicles on the job (e.g., taxicab and bus drivers, couriers, and security truck drivers).

B. Employee Testing Practices

Most employers would consider an ideal employee to be one who is well-suited to the job, skilful, knowledgeable, honest, hard working, dependable and healthy. An employer's ability to assess these qualities or attributes is dependent upon how much and what the employer knows about an individual. Traditional information-gathering techniques include job application forms, resumes, personal interviews, performance appraisals, observation by supervisory staff and reference checks. These methods provide a limited, and often subjective, body of information on a prospective or current employee. Advancements in technology, medicine, and the social sciences have led to the development of a number of new employee testing practices. Today, employers are relying on these techniques to supplement their knowledge about an individual. Among these practices are drug, genetic, lie detector and psychological testing.

i) Drug Testing

Drug testing is a general term used to describe a number of different methods of determining if an individual is currently using drugs or if an individual has used such substances in the recent past. Drug tests can detect the use of alcohol, prescription and over-the-counter drugs as well as illicit drugs.

In the workplace, drug testing may occur at a number of stages of employment and for a number of different purposes: for pre-employment purposes to screen applicants or before the successful candidate is offered a job; during employment after an accident; after an employee has been recalled to work following a leave or lay-off; when a worker exhibits unusual behaviour; or during a regular medical check-up. Drug testing may be mandatory or voluntary; random or universal.

Urinalysis is the preferred way of screening for drug abuse. This test requires an individual to provide a urine sample for analysis. Urinalysis may reveal a person's medical history, the diseases to which he or she is susceptible, what he or she ate and drank, as well as what drugs the individual has taken within a given period before the test was conducted.[35]

Blood tests are another form of drug testing. Unlike urinalysis, blood tests can only detect those drugs active in the body at the time of the test. Saliva may also be analyzed for the presence of drugs. Breathalyser tests are used to detect the presence and concentration of alcohol in the blood. Another, but less frequently used, drug test involves the radiation of a hair sample. Some think that this type of test is even more reliable than urinalysis as it reveals what drugs have been taken, and unlike urine tests, indicates when the chemicals were ingested.[36]

In the United States, corporate drug testing increased 22 per cent in 1991 from 1990. This is significant given that in 1990 it was estimated that nearly two-thirds of the major American companies already used some form of drug testing. The 1990 figures represented an increase from 50 per cent in 1989 and nearly three times the number in 1987.[37]

ii) Genetic Testing

As with drug testing, the term genetic testing refers generally to a number of techniques used to examine the genetic make-up of an individual and to determine the existence of inherited genetic traits or environmentally induced genetic changes. Genetic research has revealed that certain genetic traits may predispose an individual to a disease or may make an individual more susceptible to diseases caused by exposure to certain chemicals or toxins. To conduct genetic tests, the test subject must provide a sample of bodily tissue or fluid so that the deoxyribonucleic acid (DNA) may be analyzed. Two types of tests are generally used in the workplace:

- **Genetic monitoring** focuses on environmental workplace hazards that may affect a worker's genetic material. Its purpose is to determine whether, and to what extent, an employee may have been harmed by exposure to on-the-job toxins or other chemicals.[38] Monitoring involves the periodic examination of employees to detect the effects of toxic substances or byproducts, and to evaluate the genetic damage caused by such substances. It is used to determine if genetic material changes over time.[39]

- **Genetic screening** involves the pre-existing genetic make-up of individuals being examined to identify certain inherited traits or disorders. Unlike monitoring, which takes place over time, a single test is required for genetic screening. Screening is used to identify susceptibility to toxins, the purpose being to ensure that workers with a hypersensitivity do not undertake jobs where they might be exposed to these substances. Screening can also be used to identify general inherited conditions (e.g., Huntington's disease) that are often not directly associated with occupationally-related diseases.

Genetic testing is a relatively new technology. A recent American survey determined that only a fraction of Fortune 500 companies are currently subjecting job applicants and employees to genetic testing.[40] However, the likelihood of increased use is great, particularly as considerable research effort is being directed toward identifying all components of human genetic material or genome.

iii) Lie Detector Testing

Lie detectors are devices designed to measure the test subject's physiological responses in an effort to determine if the individual is telling the truth. This form of testing is predicated on the principle that people experience different physiological responses when they are lying and under stress, than when they are telling the truth.[41] The *Employment Standards Act*, which prohibits the mandatory use of lie detector tests in Ontario (see Part 3 for details), defines a lie detector test as:

> **46.** … an analysis, examination, interrogation or test taken or performed by means of or in conjunction with a device, instrument or machine, whether mechanical, electrical, electromagnetic, electronic or otherwise, and that is taken or performed for the purpose of assessing or purporting to assess the credibility of a person.

Polygraphs are the best known and most often used type of lie detector. Polygraphs measure three neurological responses to stress: respiration, galvanic skin response and pulse rate. Another type of lie detector is the voice stress analyzer, also known as the psychological stress evaluator. It is thought that when subjects believe they are in danger of punishment or are engaging in deception, they will have stressful reactions that suppress certain normal frequency modulations in their voices. The voice stress analyzer measures this frequency modulations. Like the polygraph, the voice stress analyzer can only detect stress, not deception.[42]

iv) Psychological Testing

In general terms, this type of testing is designed to measure an individual's psychological traits or attributes. Tests used by employers "range from aptitude testing involving simulated 'work-sample' problems to complex exams designed to determine a job applicant's primary character and personality traits."[43] Employers use psychological testing in pre-employment screening to eliminate applicants who exhibit undesirable tendencies or lack traits/skills deemed essential to successful job performance.[44] Five main types of tests are used for employment purposes:

- **General intelligence tests** measure general abilities such as verbal skills and other mental abilities.
- **Aptitude tests** are more specific and measure relatively homogeneous and clearly defined abilities[45] such as artistic, musical, and mechanical aptitudes.
- **Performance tests** are designed to measure how much an individual knows about a kind of work.[46] They are also used to determine how well or fast an individual can accomplish a task.
- **Vocational interest tests** compare a person's interest patterns with the interest patterns of people successfully employed in a specific job. The rationale behind these tests is that, if an individual exhibits the same interest patterns as those individuals successful in a given occupation, the chances are high that the individual will be satisfied in that occupation.[47]
- **Personality tests** are designed to measure characteristics such as an individual's emotional state, self-confidence, interpersonal relations, motivation in tests and attitudes.

The use of written honesty tests, a particular type of psychological testing, seems to be on the rise. These tests are designed to determine individuals' integrity and measure their attitudes towards theft. They contain questions designed to measure an individual's willingness to steal and whether they condone or rationalize dishonest behaviour. Other questions are designed to determine whether test subjects are lying in an attempt to "outsmart" the test.[48]

Handwriting analysis is also being used by organizations today. These tests are designed to assess the personality and character of the subject, including level of emotional responsiveness, mental processes, social responsiveness, approach to achievement, levels of honesty, attitudes toward life, and levels of imagination, determination, and attention.[49]

C. Employment Records

There is no standard definition of "employment records." Employers maintain personnel files and other types of records on their employees for a wide variety of reasons. Some information relates directly to employment (e.g., job applications, performance reviews, and attendance records). However, employment records may also contain sensitive information such as credit ratings, letters of recommendation, confidential medical information, reports on suspected or actual misconduct, workers' compensation claims, and sick leave.[50] Additional types of information that organizations may collect on their employees include employee ratings, comparisons with co-workers, staff development plans, management opinions of workers, future promotion chances, names of qualified replacements, and employee suggestions.[51]

D. Employer Rationale

Increasingly, employers are turning to technology to solve some of the problems they face in the workplace. Testing and surveillance techniques are viewed by employers as effective and essential management tools that can contribute to achieving goals like increased productivity or reduction of substance abuse problems in the workplace. The following discussion outlines some of the main reasons given for introducing electronic monitoring and employee testing into today's workplace. In addition, a few of the main purposes for collection and use of employment records are presented.

i) Increased Efficiency and Productivity

Productivity is one of the main reasons cited by employers for introducing electronic surveillance and employee testing to the workplace. Employers believe that corporate survival demands continuous improvements in employee productivity. Errors, poor products, and slow service hurt business. Therefore, monitoring and testing to identify and correct these problems are considered to be sound management practices.

Electronic monitoring is thought to be an effective technique for increasing employee productivity since it provides managers with information on rates of production and identifies problems impeding production and possible ways of improving efficiency.[52] It also enables management to supervise workers more effectively and to provide feedback on employee performance.[53]

Inadequate controls and procedures are considered "fundamental problems all organizations must guard against."[54] In an attempt to gain greater control over the work process and to ensure quality of product and service, employers are looking to various electronic monitoring techniques for assistance.

> Today, groups defending management's right to rely on computerized work-measurement systems note their relevance and importance to effective quality control. Those who extoll [sic] the value of secret telephone monitoring assert that listening in on conversations is necessary to assure that correct information is disseminated on behalf of the employer and to protect both parties to the transaction.[55]

It has been estimated that most costly losses incurred by organizations result from human error, accidents, and omissions. An estimated 50 to 80 per cent of annual dollar losses is attributed to error and oversights by employees.[56] In an effort to create a more productive and efficient workplace, some employers are turning to employee testing, particularly at the pre-employment stage, to "weed out" undesirable or potentially costly employees. Healthy, drug-free, honest and competent workers are seen to be the most productive and least costly in terms of absenteeism, high insurance or compensation costs, and safety problems.

ii) Alcohol and Drug Abuse

Another primary reason employers are turning to electronic surveillance and drug testing is a perceived rise in alcohol and drug abuse in the workplace. Studies show that employees with drinking or drug problems are absent 16 times more than the average employee, have an accident rate that is four times greater, use a third more sick benefits, and have five times more compensation claims while on the job. Forty per cent of industrial fatalities and 74 per cent of industrial injuries can be traced to alcohol abuse.[57]

Employers view workers with alcohol or drug problems as poor performers and are concerned that workers with substance abuse problems will cause a deterioration of employee morale, and a decline in the quality of products and services.[58] In addition, substance abuse is thought to spread to other employees once drugs are introduced into a work unit.[59]

It has been estimated that substance abuse creates security problems in the workplace, ranging from theft and destruction of company property, to the compromising of individuals in sensitive positions. Theft of company property and embezzlement of company funds are considered common ways for users to support drug habits.[60]

In 1988, the Royal Canadian Mounted Police released a study on drugs in the workplace and concluded that while there were no federal statistics on the extent and costs of drug abuse in the Canadian workplace, the results of a number of provincial and American studies suggested "significant levels of use and related problems."[61] The cost of substance abuse by employees to companies in Ontario alone was estimated to be more than $1 billion annually.[62] In Alberta, tests of workers killed in industrial accidents indicated 4.7 per cent with a blood-alcohol level (BAL) of 0.08 per cent or more, 16.5 per cent with measurable BAL's, nine per cent with evidence of prescription drugs, and 2.3 per cent tested positive for marijuana.[63]

A 1990 study estimated that the annual cost of substance abuse to the Canadian economy was $2.6 billion. However, the Alliance for a Drug-Free Canada indicated that the figure was closer to $6 billion. "Direct costs are mainly the result of absenteeism and higher health care levies for employees, while indirect costs include reduced productivity, low employee morale and customer dissatisfaction."[64]

Some employers are frustrated with the costs arising from employee use of drugs and alcohol and because of the time and resources required to get employees to acknowledge their illness and take advantage of assistance programs. The economic impact of substance abuse, together with concerns about health and safety, have moved some employers to focus on early detection and identification of "problem" workers by using testing and monitoring techniques.[65]

Some supporters of drug testing and electronic monitoring also maintain that the mere existence of these practices will act as a deterrent. They claim that employees would be less likely to use illicit drugs if they knew a program to test for drug use or to monitor employee behaviour exists.

iii) Employee Theft

Another major factor cited by employers to justify the use of electronic monitoring and testing is the prevalence of employee theft. In today's workplace, internal theft encompasses more than just pilfering of company supplies. Employers are now very concerned about the theft of confidential information, trade secrets, unauthorized (i.e., personal) use of company resources and "time theft." According to the United States Chamber of Commerce, about 60 per cent of all business failures in America are due to internal theft.[66]

No one knows exactly how large this problem is but there is a growing perception among employers that theft by workers is on the rise. In 1979, it was estimated that one in seven Ontario firms experienced serious problems with employee theft and sabotage. In 1983, according to private investigators who specialized in this area, employee theft was increasing in Canada. In fact, it was estimated that internal theft in Canada added up to more than $500 million annually. At the time, chartered accountants and security officers said that figure was conservative because many companies, particularly banks and other financial institutions, were reluctant to admit publicly that the problem existed.[67]

Some companies are now trying to control "stolen time" — paid-for hours lost to time-consuming activities unrelated to the job.[68] In 1981, a Toronto-based consultant conducted a survey of 200 Canadian employers and estimated that the average employee stole three hours and 50 minutes of time a week from his employer through lateness, early departures, phoney sick days, daydreaming, and other forms of "lolling around." Using that figure as a base estimate, the consultant estimated that this "time theft" was worth $11.5 billion to Canadian businesses.[69] By 1984, that estimate was revised upward to $15.1 billion lost to time theft.[70]

Employers use polygraphs and written honesty tests to determine if a job applicant or employee is truthful. In the case of honesty tests, some researchers argue that the best way to predict who will steal is to determine who has a favourable attitude towards theft. They maintain that people who tolerate stealing by others or who would punish thieves lightly are more likely to steal than those people who are intolerant of dishonest acts.[71]

Many forms of electronic surveillance are considered effective methods of combating employee theft. A Ministry of Labour study indicated that Ontario employers were increasingly convinced that electronic surveillance systems were the most effective and least expensive solution to the growing problem of material losses.[72]

The security of computer assets (i.e., hardware, software, programs, and data) is high on the list of employer concerns. Computer security experts divide the threats to information systems into two main categories. "Insider" threats are estimated to account for 70 to 80 per cent of the annual dollar loss, with 20 per cent of that coming from dishonest or disgruntled employees.

In comparison, "outsider" threats are negligible, accounting for only one to three per cent of losses.[73] The relative importance of risk leads employers to consider employee monitoring as the first line of defence in the protection of computer and information resources.

One of the most controversial areas regarding monitoring relates to e-mail as employers are now monitoring these messages to determine their content and destination. Supporters of such surveillance argue that employees who use e-mail to send frivolous messages or to run their own businesses are using up company resources both in terms of computer capacity and employee time. Therefore, monitoring is justified to determine how a company's resources are being used.[74] This argument recently received support in a California court decision. In August 1990, a class action suit was filed in Los Angeles against Epson America, Inc. The company was charged with violating employees' privacy by intercepting their e-mail messages. The judge ruled that monitoring e-mail was not the same thing as electronic eavesdropping, which is a violation of the California penal code, and that companies have the right to manage their e-mail systems. While this decision has been appealed, the implication is that e-mail is not private and that firms own any data developed on company-owned equipment or company-purchased services.[75]

iv) Health and Safety

In Ontario, under the *Occupational Health and Safety Act*, employers are required to ensure the health and safety of their employees at the workplace. Other statutes, such as the *Health Protection and Promotion Act*, require certain employers to take additional health precautions. Given that employers have legal responsibilities under these statutes, many argue that the collection of medical information, as well as the use of employee testing and electronic monitoring is justified if these practices are used to prevent accidents and to protect the health of workers and the public.

Supporters of drug testing maintain that it is very useful in protecting the health and safety of employees, as well as the public, as it can identify impaired workers in safety-sensitive positions. Concern about safety was one of the main reasons given for the introduction of the drug testing program at a major Canadian oil company on January 1, 1992. Under the company's plan, employees who want to work in areas where safety is an issue must undergo a urine test for drug use. If they refuse, their wages can be frozen for five years and they can be moved to another job. The plan also requires all job applicants to be tested as a condition of employment.[76]

Health and safety concerns are, essentially, the only legitimate reasons for introducing genetic testing into the workplace:

> It is technologically and economically impossible to lower the exposure to hazardous agents to zero. However, if individuals or groups who were predisposed to specific types of occupational illness could be identified, other preventative measures could be specifically directed at those persons.[77]

As testing may identify susceptibility to a disease, it can provide both employer and employee with useful information to ensure that predisposed individuals are not placed in jobs where they could be exposed to certain workplace hazards or toxic substances.

v) Routine Personnel Matters

In order to function properly, it is necessary for any organization to keep records relating to its employees. Employee information is needed for administrative purposes as well as to fulfill statutory requirements. Personnel records serve a number of specific purposes including decisions regarding hiring, firing, transferring, promoting, demoting, training, disciplining, and the provision of benefits to employees. Information may also be relevant to safety issues. An employer is under statutory and common law duties to ensure the safety of employees and of third parties.

Another reason for collecting personal information on an employee is to determine whether an individual is fit to perform a particular task. Medical test results are a prime example of this type of information. According to employers, it is unsafe, inefficient and unjustifiable to require them to set work tasks in ignorance, when the opportunity exists to proceed in an informed fashion.[78]

As data is collected regarding these various decisions, a broad base of recorded information about an employee is created. Thereafter, a variety of individuals and organizations unrelated to the employer-employee relationship may consider this information to be a valuable resource (see Part 2 for discussion of informational privacy concerns).

vi) Health Costs

In the United States, the high cost of health insurance is a powerful reason motivating employers to introduce employee testing into the workplace. "As medical expenses whirl skyward, more companies have begun to see smokers, drinkers, and workers who engage in other 'high risk' — but legal — activities as a burden."[79] Organizations are concerned about how a worker's "unhealthy lifestyle" could affect their health care costs. This has prompted employers to collect and maintain more personal information than was previously the practice. Employers want to determine if an individual smokes, drinks, is obese, or participates in high risk after-hour hobbies. For example, one American city requires job applicants to sign affidavits certifying that they do not smoke, and have not for a year. Another municipality in the United States used to require all job applicants to take a cholesterol test and then eliminated those candidates whose levels were in the highest 20 per cent.[80]

In Ontario, employers are concerned about rising workers' compensation premiums and the penalties resulting from high accident rates and unsafe work environments. In an effort to reduce these costs and create a healthy and safe workplace, Ontario employers use employee testing to identify workers with substance abuse problems.

vii) Employer Liability

The courts in Canada have held that employers are generally liable for damage done by the fault or negligence of their employees acting in the course of employment. This is based on the concept of "vicarious liability". An employer can also be found to be personally liable for damage caused by an employee through employer negligence. For example, an employer might be found to have carelessly entrusted work to someone who is incompetent, or the employer could have known that there was a risk of harm unless special precautions were taken, and failed to give instructions accordingly.[81] Finally, some Canadian employers have been held liable for negligent misrepresentations made by their employees.

As employers are strictly liable for many of the actions of their employees, they have a great incentive to lessen the likelihood of hiring negligent individuals. Therefore, employers are utilizing whatever means available, including employee testing and electronic monitoring, to protect themselves.

viii) Benefits to Employees

Proponents of employee testing argue that such tests may also benefit the affected workers. By identifying impaired individuals, drug testing is thought to help reduce workplace accidents to the benefit of all employees. Polygraph testing can assist individuals who are suspected of wrongdoing by providing them with an opportunity to clear their names. By volunteering to take a polygraph test, employees can demonstrate their willingness to prove that they are honest, reliable and trustworthy.

Supporters of electronic surveillance have put forth similar arguments. Monitoring introduced for one purpose may also provide peripheral benefits to affected employees. For example, the permanent records from monitoring can protect the innocent from false accusations and can document violations by the guilty. Video cameras designed to prevent theft from loading areas may increase safety in adjacent parking lots.[82]

ix) Employers' Rights

In addition to all the reasons why employee testing, electronic monitoring and employment information are useful to a business, employers maintain that it is their right to introduce whatever practices they think necessary into their workplace. With regards to electronic surveillance they have argued that:

- monitoring is generally done on the employer's premises by equipment owned by the employer;
- the employee activity that is subject to scrutiny is typically performed in the open, either in group settings or in semi-private situations; and
- monitoring through electronic means is not substantially different from supervision exercised in many employer-employee relationships.[83]

Use of electronic monitoring has also been justified as "an exercise of a property right." Employers view surveillance as necessary to promote security, safety and productivity. They believe that to regulate or prohibit electronic surveillance would abridge their rights and damage their business.[84] The same sorts of arguments have been advanced for employee testing. Finally, employers note that if a worker objects to any workplace practice, the employee is free to terminate the employment relationship.

E. Objections to Electronic Monitoring & Employee Testing

Privacy and worker advocates acknowledge employers' right to protect their own property, but contend that this right does not supersede all the rights of employees. They feel that employers do not have the right to demean or abuse their employees:

> … since the values, needs and intelligence of people do not change when they enter the workplace, there is no reason why the rights and responsibilities they enjoy as citizens should be withheld from them in their role as workers.[85]

In addition, advocates question some of the conclusions employers have reached as to the effectiveness of employee testing and electronic monitoring. The following is a discussion of several of their general objections to what they consider to be intrusive employment practices (for privacy concerns, see Part 2).

i) Counterproductive Measures

Privacy advocates contend that employers often introduce electronic monitoring on the assumption that it will improve productivity, but without any real understanding of how. Observers maintain that despite increased adoption of monitors, businesses are actually ill-equipped to anticipate their potential effectiveness. Many companies install a monitor when they introduce a new computer application system or improve an existing one. This makes it difficult to separate the results of monitoring from those of work process changes.[86]

A study on the use of computer monitoring in select Canadian firms concluded that the use of monitors does not automatically improve attention to productivity.[87] In fact, anecdotal evidence shows that over-zealous electronic monitoring can be counter-productive.[88] At the Workshop on Information Technologies and Personal Privacy in Canada, one participant noted that intense surveillance of workers by electronic means to determine quantity of work, fails to take into account the human aspect of work. Quality is replaced by quantity.[89] The results of a survey conducted by the Massachusetts Coalition on New Office Technology, from 1987 to 1989, supported this conclusion. Respondents said that with electronic monitoring the quality of service suffered, employee satisfaction declined, and work was not measured fully and fairly. The consequence was that productivity suffered as well.[90]

Monitoring can also create adversarial relationships in the workplace that may lower productivity over time. Privacy and worker advocates believe that employees may feel violated and powerless in the face of the new electronic monitoring techniques. This may result in destructive countermeasures and even an increase in the violations or abuses monitoring is intended to stop. Workers may feel challenged to beat the systems by disrupting, distorting or deceiving the monitors. For example,

typists may hold one key down to increase the number of keystrokes recorded. They can delete the file containing the errors at a later time. Telephone reservationists may avoid calls that add to their average call time, by either disconnecting the call or withholding additional information from the caller.[91]

ii) Health and Safety Issues

Opponents of employee testing and electronic monitoring, while not attempting to minimize the significance or consequences of substance abuse, do question the reliability of the figures cited to support the conclusion that alcohol and drug abuse in the workplace is on the rise. In addition, some think that drug testing and surveillance are not effective or appropriate methods of identifying or combating substance abuse.

> Drug testing disguises the real health and safety problems in the workplace. Fingering drug testing as a solution to workplace accidents allows employers and governments to ignore the much more frequent sources of dangers at work. Stress, long working hours, poor enforcement of existing health and safety laws, inappropriate or dangerous equipment and toxic materials are all more common causes of accidents and illnesses to workers, but because employers bear responsibility for these matters, they are rarely talked about.[92]

iii) Extensiveness of Monitoring or Testing

Opponents object to the extensiveness of electronic surveillance used to protect computer and information assets and recommend that security measures be limited in their application. Some maintain the rapid growth of the information security field and the considerable publicity about computer crimes has fostered many myths. They believe that there are no valid statistics on the costs of computer crime. Additionally, while acknowledging that more losses do occur from authorized persons engaged in unauthorized activity, opponents think that attempting to distinguish the degree of risk posed by insiders and outsiders "oversimplifies complex relationships between victims and perpetrators."[93] Worker and privacy advocates contend that electronic surveillance may give the employer the benefit of increased security, but the practice exacts a price from all employees in terms of loss of privacy and human dignity.[94]

Privacy and worker advocates also think that employers should look for ways of minimizing the intrusiveness of practices such as electronic surveillance. For example, employers could consult the affected workers on ways of reducing intrusiveness before a practice is introduced, electronic surveillance could be conducted in an overt rather than covert manner, or employees could be given access to their own performance data. Intrusiveness may also be addressed in the design of an

electronic monitoring system. Some employers do not consider it cost effective to use call management systems to evaluate every call. Rather, "exception" reports are generated when there is an unusual call pattern. Software is used to select and report on calls that have a high likelihood of being unofficial (e.g., calls to audio text numbers, calls at unusual times or to unusual destinations, long or reoccurring calls).[95]

There are also technologies that may be used to reach the desired end-result, but that do not involve employee monitoring. Telephone systems can be programmed to restrict the type of calls that may be made from certain telephones. In this manner, telephones in departments that do not deal with the public can be programmed to only make in-house calls. Telephones of workers with no out-of-town business can be programmed to provide only local service.[96]

Concerns over extensiveness have also been raised with regard to employee testing. Perhaps the area that has received the most attention is mandatory drug testing. Aside from the argument that this practice is an invasion of workers' privacy (see Part 2), opponents question whether or not it is necessary to unilaterally subject all employees to testing (universal testing) when there may not be reasonable grounds to believe that alcohol and/or drugs are being brought to or consumed at the workplace.[97]

Opponents of these workplace practices think that the manner of application largely determines the fairness of the practice and the degree of intrusiveness. They encourage employers to look for alternatives and to consider the issues of quality of work life, employee participation, fairness, and equity when introducing employment practices.

Part 2 — Privacy Concerns

As discussed in the preceding section, employers report that they do not collect employee information or undertake testing and monitoring for frivolous reasons. Rather, these expensive and time-consuming practices are considered appropriate management tools designed to address legitimate issues. Regardless, privacy advocates maintain that these practices are highly intrusive and a threat to worker privacy. They "pit the need of the company against the worker's feelings of dignity and worth."[98] Also, as many practices are not regulated by law (see Part 3), they are seen to be open to abuse.

Outlined below are the significant privacy concerns related to electronic monitoring, employee testing, and the misuse of employment records.

A. Loss of Personal Autonomy

The potential loss of personal autonomy for affected workers resulting from intrusive employment practices is a central privacy concern. Simply stated, autonomy is "the quality or state of being independent, free and self-directing."[99] Autonomy may be limited or compromised for reasons such as the use of direct or implied coercion, or where circumstances limit one's ability to act knowledgeably in one's own interest. Some privacy advocates maintain that workers may be restricted in their full expression of autonomy as: "Preordained rules of behaviour, job requirements, limited resources or information, and concern over job security can limit autonomy."[100]

In a study of drug testing, the former Privacy Commissioner of Canada stated that drug testing coerces conformity and restricts autonomy.[101] The argument is clearly applicable to genetic testing as well:

> … preemployment tests that presumably identify genetically susceptible individual may be used to restrict the type of job an employee is permitted to undertake or to ban the worker from employment in the industry altogether. Similarly, testing done during employment, which detects early warning indicators of possible future disease, might be used preemptively to remove employees from a given station or set of job duties. Each of these steps, if taken unilaterally by an employer, could be seen as a restriction of the autonomy or liberty of the individual worker to elect a suitable job and/or to accept the attending risks.[102]

Surveillance technology is now so highly developed that every possible variable that can be measured is monitored. As an American bank vice-president noted, when commenting on the 200 criteria he used to assess productivity among workers in his credit-card division: "I measure everything that moves."[103] This continuous and extensive monitoring of employees' activities severely restricts worker autonomy. In addition, if an employer uses the information gathered through surveillance to change the pace or style of work, an employee may lose further control over his or her own job.[104]

B. Lack of Consent

Employment practices such as electronic monitoring or employee testing may be introduced without consultation with affected employees. In these instances, workers are not given the opportunity to consent to the practice or to the subsequent collection of their personal information. Consent means voluntary agreement, the act or result of coming into accord. It is an act that is unclouded by fraud or duress.[105] In the context of the employer-employee relationship, some privacy advocates question whether true consent is possible. Even if a worker agrees to a practice, the perceived or stated consequences of refusal (e.g., relocation, suspension or termination) places the employee under duress thereby making consent, in the full meaning of the term, impossible.

> Can there be any doubt that the employer exercises power of life and death over each of us at least as great as the power of government? The power to deprive us of our livelihood, often with no notice. … The power to lay off, to transfer to an undesirable community, to reassign to an unhappy job. The power to make us miserable. The power to strip us of our identity, to the extent that our vocation is our identity.[106]

Some consider informed consent to be the standard required to ensure that privacy violations do not occur. This means that a person's agreement to allow something to happen is based on a full disclosure of the facts needed to make an intelligent decision.[107] A worker could consent to, for example, providing a blood sample without a full understanding of what types of tests will be run and the possible consequences of an adverse test result.

One view on the issue of consent is that an employee does not have a right to privacy during working hours. An American arbitrator, in an early decision regarding electronic monitoring, wrote:

> The right of privacy concerns an individual's right not to have his statements, actions, etc., made public without his consent. But this serves only to protect him against the publication of his PRIVATE statements or PRIVATE actions. It should be evident that an employee's actions during working hours are NOT PRIVATE actions.[108]

Although the right to privacy in the workplace has now been established by Canadian arbitration cases, the view that consent for monitoring is automatic with the establishment of an employment relationship, unless otherwise specified in an employment contract, government legislation, or elsewhere, is still prevalent among some employers. However, privacy advocates argue that employees do not automatically extend consent to electronic surveillance or any other employer action that may reduce privacy.[109] In its 1987 report on the review of the Canadian federal *Access to Information Act* and *Privacy Act*, the Standing Committee on Justice and Solicitor General concluded that all employees should have "the right to consent to work in a heavily-monitored environment and to be consulted about the uses of data derived from any surveillance process."[110]

In practice, consent is not always sought by employers, particularly if they want to conduct electronic monitoring in a covert manner. Secret monitoring is considered to be a clear invasion of

privacy. Objections to covert monitoring have also been raised by workers and unions on the grounds that the practice is sometimes used to control or intimidate workers.[111]

There is also concern about the privacy rights of third parties. For example, when an employee is subjected to telephone service observation, the caller is also monitored. Often the caller is unaware that there is another individual listening to the call or that the call is being taped. Therefore, the caller is not in a position to consent to the monitoring. For this reason, some forms of electronic monitoring are considered to invade the public's privacy as well as that of the affected employee.

Employee testing may also be conducted in a covert manner without a worker's knowledge or consent. For example, handwriting analysis may be done from any sample submitted during the normal course of business. Blood and urine samples provided during a regular company medical may be used to conduct drug and genetic tests without the employee's knowledge. It is may soon even be possible to collect and test urine entirely without the individual knowing.[112]

C. Invasion of Privacy of Person

One of the most critical privacy issues relating to both drug and genetic testing is that they are seen as an invasion of the body and a direct violation of privacy of person.

> … urinalysis is highly intrusive. It not only requires the surrender of a body fluid, but, to prevent the subject adulterating or substituting the sample, it may be necessary to observe the subject's genitals as he or she urinates. The disposal of body wastes is generally considered a highly personal act. Urinalysis may expose this act to close visual scrutiny. Such observation is intrusive and humiliating.[113]

Mr. Justice La Forest, of the Supreme Court of Canada, highlighted this privacy concern by noting that: "… the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity."[114]

D. Invasion of Informational Privacy

Central to the concept of informational privacy is the ability to determine when, how, and to what extent information about oneself is communicated to others.[115] While the issue is not confined to the workplace, some maintain that loss of control over personal information is perhaps the most significant of all privacy issues:

> … not only does the loss of control of information about one's self have some possible serious negative consequences, such as no protection from misuses of the information, it also means a loss of autonomy… Loss of autonomy means loss of one's capacity to control one's life… A right to control information about one's self is fundamental to being a self-determining and responsible being.[116]

This sentiment was echoed in the report from the 1985 Workshop on Information Technologies and Personal Privacy in Canada:

> The consequences of losing control over personal information go beyond the issue of invasions of privacy. A fundamental aspect of life is being endangered — the freedom to be oneself and the freedom to speak and act. If people think or know that their activities are being monitored or recorded, they tend to act cautiously to protect themselves, and may even start to censor their thoughts and actions. Therefore, the issue of privacy is related to the much larger dimension of personal and political freedom.[117]

The code of fair information practices is an internationally recognized standard for the protection of data and informational privacy. The code states that:

- There must be no personal data record-keeping whose very existence is secret.
- There must be a way for a person to find out what information about him is in a record and how it is being used.
- There must be a way for a person to prevent information about himself that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for a person to correct or amend a record of identifiable information about himself.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[118]

In Ontario, these principles are codified in the *Freedom of Information and Protection of Privacy Act* and in the *Municipal Freedom of Information and Protection of Privacy Act*. Many of the privacy concerns surrounding practices like testing or monitoring revolve around potential violations of the code of fair information practices.

i) Collection of Unnecessary or Irrelevant Personal Information

As noted, companies maintain records on their employees for a variety of reasons. Some employers think it is their right to collect and use whatever information about their employees they want or need. While this collection may be viewed as an intrusion by the workers, employers may see it as a condition of employment.

Job application forms raise potential privacy problems as they frequently collect information that is not required until after the applicant is hired, or information that an employer has no need to know at all. Examples of this type of information are:

- arrest records, upon acquittal or when formal charges have been dropped;
- investigative material regarding a civil, criminal, or administrative wrongdoing by an employee that resulted in the employee's acquittal;
- political or religious affiliation.[119]

Investigation of prospective employees is another practice that may involve the collection of unnecessary personal information. A 1989 survey of Fortune 500 companies employing 3.7 million people determined that 57 per cent used private investigative agencies to collect or verify information about employees; 42 per cent collected the information without telling the affected individual.[120] Investigators may speak with neighbours, current and former business associates and other acquaintances. Some of the information collected is of a personal nature and not relevant to the job in question. This practice is particularly problematic when information is "supplied by vindictive, jealous or cantankerous neighbours or business associates" and the data subject is not given an opportunity to know what information was collected, or to refute it if it is false.[121]

Collection of extraneous personal information has been exacerbated by advances in technology. The increased capacity of computers to collect, retain and manipulate information has raised longstanding concerns related to collection and retention of personal information to new heights.

> The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer.[122]

Collection of unnecessary personal information is of particular concern with electronic surveillance. A participant in the 1985 Workshop on Information Technologies and Personal Privacy in Canada reported that the following private conversations of three different employees in an airline reservation office were recorded through voice-activated microphones in the telephone headsets they were wearing:

- a reservation agent paused during her work to tell her friend, sitting next to her, that she had cancer of the cervix;
- another employee placed a call to his companion — both were homosexual;
- a third employee chatted to a friend during his last half hour of work about his planned afternoon at a nearby nudist beach.

These employees were unaware that their conversation had been monitored. The two male employees found out their privacy had been invaded when supervisors replayed the tapes of their conversations during performance appraisals. The female employee became aware of what had transpired when she was consoled by her supervisor about her illness. The supervisor also discussed

her health problems with others in the office.[123] These examples illustrate how the collection of non-work-related personal information can harm people by revealing intimate details about their personal lives.

The problem of collecting too much or irrelevant information has two components. First, opinions differ between employers and employees on what information is necessary to accomplish a given purpose. Second, there are technical difficulties in separating legitimate information from what could be called "private" information. For example, video cameras directed at a production area monitor the production process as well as every movement of the employees. Filtering out the unnecessary personal information is considered impossible with this type of electronic monitoring.[124] Another problem derived from the new technology is that, once a monitoring or computer system has been established, the cost of collecting and storing additional information is minimal. Therefore, there is a tendency for organizations to gather more information and discard less.

Similar problems exist for certain types of employee testing. Often collection of unnecessary or irrelevant information is symptomatic of the nature of the tests. This is the case for urinalysis. The use of certain prescription drugs (e.g., some of the drugs required to treat heart conditions, epilepsy, diabetes or asthma),[125] as well as some over-the-counter products such as Alka-Selzer Plus, Allerest, Contact, Nyquil, Primatene, Sinutab and Sudafed, can produce positive test results.[126] In order to explain the "false positives" that result, employers may require test subjects to list all drug products taken in the weeks preceding the test. In this way, individuals may be required to disclose personal information relating to their health, diet and personal habits that are not relevant to the purpose of determining the use of illicit drugs. Other tests may also reveal personal information that is not relevant to the job (e.g., a blood or urine test may reveal if a female worker is pregnant).

ii) Monitoring of Non-Work-Related Activities

Collection of information on employees' non-work-related activities is not a new practice. Automobile-maker Henry Ford's "Social Department" sent investigators around to the homes of assembly line workers to discover their marital situation, number of children, religious and ethnic backgrounds.[127] However, there are new concerns that advances in testing and electronic monitoring enable employers to collect far more personal information on employee after-hour activities than was previously possible.

Privacy and worker advocates are concerned that testing technology, particularly urinalysis, enables employers to transcend barriers that traditionally protected privacy. Some drugs remain in the body long after they have been ingested. As urinalysis cannot determine exactly when a drug was used, employers are able, to some extent, to collect personal information about an employee's non-work-related activities (e.g., that a worker had a drink or smoked marijuana on the weekend). This means an employee's home is no longer his or her private domain because activities conducted there may be identified and used against the employee on the job. This is seen as an attempt to control employees' private lives[128] and is considered to be, in essence, an invasion of territorial privacy.

Electronic vehicle tracking is one form of electronic monitoring that is capable of revealing information about a person's lifestyle, relationships and affiliations. If an employee uses a company vehicle for non-work-related activities and monitoring by the company is continued after hours, it would be possible to deduce the following information from a vehicle's movements:

- when the employee is at home;
- where the employee spends his/her leisure time;
- where he/she shops;
- which school the employee's children attend;
- which church the worker attends;
- where the employee's friends, relatives and associates live;
- whether the worker visited a doctor, a psychiatrist, or drug counsellor;
- which political meeting or union rallies he or she attended; and so on.[129]

iii) Inaccuracy of Personal Information

Another informational privacy concern relates to the accuracy of information collected by the employer and the validity of the conclusions based on that information. Under the code of fair information practices, the reliability of data should be assured and precautions taken to prevent misuse of information. All forms of employee testing have a number of technical or methodological problems that limit the accuracy and reliability of the test results. Also, employers may inappropriately or incorrectly administer a test, or they may not fully understand the capabilities of a test and draw erroneous conclusions as a result.

As noted, urinalysis cannot identify the quantity of a drug ingested or the time it was taken. Cocaine may be detected in urine up to three days after consumption. Trace chemicals may be present from five days to three weeks after marijuana use.[130] Therefore, it is incorrect to conclude that a urinalysis test can detect current drug use with certainty. Urinalysis can merely identify usage that has occurred within a period before testing.[131]

Also, most drug tests are unable to determine the extent to which use of a drug results in impairment, interference with job performance, or presents a true safety threat. Tests cannot predict an employee's ability to perform a job since tolerance to drugs varies from person to person due to chemical, physiological or psychological factors. Therefore, privacy advocates maintain that it is impossible to accurately measure performance problems on the basis of a drug test.[132]

Methodological problems are also associated with genetic testing, but one of the biggest problems occurs when the results are misinterpreted.

> There are two types of genetic disorders: genetic diseases and genetic predispositions. In the case of genetic diseases, the genetic component is so strong that it's going to affect the individual, regardless of what he/she tries to do to avoid it … Environment doesn't play much of a role in these types of disorders. …
>
> The second group of disorders is completely different. These are the disorders with a genetic predisposition. They may or may not occur, depending on several factors. Environment is one such factor. These diseases tend to be multi-genetic, meaning that multiple genes interact and, depending on how they interact, the individual may or may not develop the disease.[133]

Diseases such as cystic fibrosis, haemophilia and muscular dystrophy fall in the former category. Coronary heart disease, stroke, hypertension, diabetes, epilepsy and cancer are classified under the latter category.[134]

Genetic testing can identify individuals with genetic susceptibilities or predisposition to a disease, but a direct correlation between predisposing factors and the development of a disease does not exist. Factors such as age, sex, race, work history, diet, smoking, alcohol and drug consumption, may affect whether or not a disorder manifests itself. As these and other factors may exacerbate or minimize the effects of predisposition, it is incorrect to conclude that possession of the genetic predisposition alone causes disease.[135]

Another reason opponents of employee testing caution that the results of genetic tests should not be viewed as absolute certainties is because there is a significant problem in identifying the relationship between hazardous work environments and occupational diseases. Due to long latency periods, it is difficult to demonstrate causal relationships between exposure to hazardous environments and occupational diseases.

> Until the health effects of radiation and chemical exposures are better understood, genetic and biological monitoring of exposed populations can only provide a gross indication that genetic changes have occurred and that adverse health effects could follow.[136]

Some people view genetic information as infallible, accurate, and highly predictive. "Nothing could be further from the truth. Genetic tests are like any other tests; there are going to be false positives and other problems."[137] Some employers may not fully understand this and may make decisions, based on the result of a genetic test, that adversely affect individuals.

Two separate American studies conducted in 1983 and 1986 concluded that polygraphs were unreliable as a general screening device. Experts attribute the inaccuracy of pre-employment polygraphs to a number of factors including the openness of questions typically asked in

pre-employment screening. Questions such as "Have you ever stolen anything?" are more likely to arouse stress in an honest person trying to answer the question truthfully but unsure of its scope, than in a dishonest person.[138] Another problem with polygraph testing is the results do not depend on the accuracy of the measuring instrument, but rather on the subjective interpretation of the examiners.

Controversy over the accuracy and usefulness of all types of psychological tests also exists, but particularly with personality tests. Some of these tests are considered highly unreliable and of questionable validity. Test subjects can either fake their responses or provide socially desirable answers. As with polygraph testings, personality tests are subjective and require a trained professional to properly interpret the results. One study revealed that there was no independent research supporting the validity of personality tests.[139]

Another concern is that personal information, such as the results of employee tests or performance statistics obtained through monitoring, may be retained longer than necessary, leaving files full of out-of-date and inaccurate information. Scores on skills-related tests may change over time as employees acquire new skills or become more proficient at old ones. This is also true for health information as workers' health can improve, their lifestyles can change and habits can be broken.

Some employers hold the view that electronic surveillance techniques bring greater accuracy to monitoring than traditional methods of supervision and performance evaluation because so many parameters of job performance can be monitored. Employees often disagree. They believe that electronic monitoring does not produce accurate information, either in terms of correctness of data, or in terms of the capability of technology to accurately capture the quality of an employee's performance.

iv) Unauthorized Use of Personal Information

Central to the code of fair information practices is that personal information should not be used for purposes other than those for which it was collected without the data subject's consent. There is an apprehension that employers will use the personal information in employment records for unethical and discriminatory purposes. This concern has been heightened due to the extensiveness of the information that can be collected through testing and electronic surveillance.

Although supporters have argued that employee testing provides "a useful function in choosing qualified employees in a non-discriminatory manner,"[140] opponents disagree. All types of testing reveal highly personal information that could be used to discriminate against the test subject.

Discriminatory use of test results is of particular concern in the area of genetic testing. Genetic testing has been called "the beginning of the new eugenics movement of the technological age."[141] The information supplied by these tests goes far beyond what is needed by employers to make occupational decisions. Genetic screening can be used to exclude individuals from certain jobs and could conceivably result in entire classes of people being stigmatized as being "genetically inferior."[142]

Once labelled, individuals may be barred from certain jobs in an industry or beyond, if the information is placed in a widely-accessible database. People in the United States and Canada with certain genetic diseases or predispositions have already been denied insurance and employment.[143] Genetic tests raise the spectre of a society divided into two classes: one that is perceived as fit and healthy and another that has been labelled "unhealthy." Those in the latter category may remain either marginally employed, or unemployed and unemployable.[144] In addition, if such labels are attached to historically disadvantaged groups, that status could be perpetuated.[145]

It has been argued that electronic surveillance alleviates any discrimination and inequity that might arise when using traditional monitoring or supervisory techniques because:

- technological monitors have no favourites and treat all employees alike; and
- certain practices (e.g., access control systems) make equal demands on all who encounter them and not just certain types of employees.[146]

Opponents note that electronic monitoring is only as objective as the person who uses the information.[147] Finally, as the majority of electronic surveillance is still targeted towards specific jobs such as clerical and telephone clerks and as these positions are predominantly held by women, these practices are also seen as discriminatory.

v) Unauthorized Disclosure of Personal Information

Employers frequently receive requests for employment information from other employers, social workers, insurance companies, credit bureaus, government officials, and union business agents. A survey of American Fortune 500 companies revealed that 80 per cent of the surveyed companies will give information to an employee's potential creditor without a court order. Fifty-eight per cent will also give employee information to landlords.[148]

Although individuals initially disclose personal information to obtain or continue employment, they do not generally consent to that information being released to others. Through these disclosures, the employee loses control of sensitive personal information as well as the opportunity to verify the accuracy of that data.[149] Disclosure of personal information for purposes other than for which it was collected, without the consent of the data subject, is a direct contravention of the code of fair information practices.

A concern raised about written honesty tests is equally applicable to all types of potentially damaging personal information collected by employers:

> A central privacy concern is that databases will begin filling up with names and test results of job applicants who "failed" the tests, and that employers and other third parties will enjoy easy access to data of questionable validity that carry the stigma of dishonesty and failure.[150]

vi) Denial of Access and Correction to Employment Records

The code of fair information practices provides that individuals should have the right of access to their personal information and be allowed to correct or amend records, if necessary.

Unfortunately, employees are not always given the opportunity to review their own employment records. This is of particular concern when these records contain the results of monitoring or testing, and the accuracy of some of this information is questionable.

E. Pandora's Box

Many privacy advocates fear that the use of intrusive employment practices will only increase as new applications are devised and the cost of the technology decreases. This has certainly been the case with electronic monitoring. With affordability has come a wide variety of new applications.

> Many of the new surveillance devices are relatively low in price, easy to obtain or to put together, simple to install and cheap to operate. Their power of perception vastly supplements that of the human ear or eye, and their ability to record lends permanence to the perception. There is, therefore, a great temptation to find new uses for such devices, to the detriment of privacy, or to use them to replace traditional methods of surveillance.[151]

Increasingly, surveillance devices automatically record data that workers generate.[152] Many believe that as electronic monitoring is now "an unobtrusive by-product" of the work process, its use is even more likely to spread.[153]

One of the key questions being asked by privacy advocates is — just because something is technically possible and affordable, does that make it necessary or useful? There is a concern that employers may get caught up with the capabilities of electronic monitoring without stopping to think whether that level of surveillance is necessary, appropriate, or ethical.

Speaking out against this type of "technological determinism," a leading Canadian privacy advocate warned against:

> … the entrepreneurial search for an application of newly developed technology and the naive quest for technical solutions to such serious social problems as low productivity, employee theft, and drug and alcohol abuse. Rather than management identifying an important issue and then turning to the technocrats for a solution, technological advances are driving the process of problem identification.[154]

Another cautionary note was sounded in the report of the Workshop on Information Technologies and Personal Privacy in Canada:

> Information technologies are commonly believed to be neutral tools that can be used for either good or bad purposes. This view ignores an important characteristic of such technologies — their inherent capacity to create environments that can fundamentally change the way individuals think and live. As Marshall McLuhan wrote, "Electronic information systems are live environments in the full organic sense. They alter our feelings and sensibilities, especially when they are not attended to."[155]

A final privacy concern is the impact that workplace practices may be having on society in general. With regard to electronic monitoring, there is an apprehension that practices developed at work will expand into other areas so that monitoring will become more extensive in society at large.[156]

> Omnipresent monitoring will almost certainly chill political and social expression. Security and control may be enhanced but at the cost of a less creative and dynamic society. If … democracy is to be destroyed, it is unlikely to happen by sudden catastrophic events. Rather, it will occur by slow, incremental changes defined in benign terms. As Justice Louis Brandeis said, "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[157]

This warning is equally applicable to other workplace practices, particularly genetic testing. History is replete with examples of developments in technology, the negative side effects of which were completely unanticipated at the time of discovery.[158]

F. *Charter* Issues

There is a concern that basic legal principles are being compromised by the use of intrusive practices in the workplace. In addition, as the government functions as an employer, several *Charter* issues could potentially arise within the public sector workplace.

i) Presumption of Innocence

The belief that each individual is innocent until proven guilty is fundamental to the *Canadian Charter of Rights and Freedoms*. This principle is embodied in subsection 11(d) of the *Charter* which gives every citizen the right "to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal."[159]

There are indications that practices like mandatory drug testing turn this presumption of innocence into the presumption of guilt. Such practices shift the burden of proof from the employer having to prove wrongdoing to the employee having to prove innocence. One observer noted that

mandatory drug testing enables "employers to use duress — holding hostage a person's livelihood — to investigate people against whom they have no evidence of wrongdoing. The individual is presumed guilty unless proved innocent…"[160]

In the context of electronic monitoring, supporters say that employers would not expend the time or money required for these practices without justification. Monitoring is merely used to identify the guilty parties. The Privacy Committee of New South Wales, Australia, has criticized this argument as just another example of the "nothing to hide nothing to fear" mentality that has been advanced by proponents of all kinds of modern surveillance systems.[161]

ii) Due Process

Due process is one of the most contentious issues regarding the lawfulness of certain employment practices. Due process means that proceedings are carried out in a lawful and just manner and that there is a right for the affected parties to challenge and refute information before a decision is made or any action taken. To the extent that some employees are not notified of employment practices, not given the opportunity to consent, not allowed access to the information obtained, and not given an opportunity to correct or refute that information before disciplinary action is taken, due process may be circumvented.

The issue of due process may arise under section 7 of the *Canadian Charter of Rights and Freedoms* which states that:

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

Two of the cases that have considered the constitutional validity of mandatory drug testing arose within a prison context.[162] Despite this focus, they may provide some indication of how the court may respond, in other instances, to claims under section 7.

A provision in the prison regulations authorized drug testing where a civil servant or employee of a penitentiary considered a urine sample necessary to detect the presence of an intoxicant.

> In addressing s. 7 of the *Charter*, the courts found that the privacy and dignity rights of prison inmates were entitled to some degree of protection and that drug testing implicated these rights. Ultimately, they held that the regulation violated s.7 because it did not accord with the principles of fundamental justice … It was too broadly framed and failed to set out any objective criteria, including reasonable and probable grounds for suspicion, for determining whether a drug test was necessary. In the absence of such criteria, inmates could be subject to arbitrary and harassing invasions of privacy.[163]

iii) Search and Seizure

Section 8 of the *Charter of Rights and Freedoms* states that "everyone has the right to be secure against unreasonable search and seizure." Some employment practices may constitute an unreasonable search and seizure. Electronic monitoring of workers is viewed by many as a "dragnet" or "fishing expedition." Its use is not triggered by specific evidence. Rather its very purpose is to generate the evidence of wrong-doing. Opponents believe that electronic monitoring, without the express and volunteered consent of the parties involved, may constitute an unlawful search and seizure under section 8 of the *Charter*.

Canadian courts have found that various forms of testing, such as blood, breathalyzer and urinalysis, may constitute a search within the meaning of section 8. Therefore, genetic, psychological, drug and lie detector testing could all potentially support challenges under the *Charter*. In one of the cases regarding the constitutional validity of mandatory drug testing of prison inmates, the court found that urinalysis constituted a search within the meaning of section 8.[164] In another case, Mr. Justice Gallpeau commented on the intrusion of privacy involved in the process of urinalysis in the following passage:

> The right to the intimacy, to the discretion, and to the secrecy of acts of private life is part of the right to the security of the person. To require that the inmate provide a sample of his urine causes him humiliation and constitutes an intrusion into the security, the tranquillity and the intimacy of his person.[165]

iv) Equal Protection

The potential for discriminatory use of personal information by employers has already been addressed under "Unauthorized Use of Personal Information." However, this issue may also arise in the context of the *Charter*. The principle of equal protection is established under subsection 15(1) of the *Charter of Rights and Freedoms* which states:

> Every individual is equal before and under the law and has the right to equal protection and equal benefits of the law without discrimination and, in particular without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

An employment practice, such as testing, that is conducted in a discriminatory manner (e.g., targeted against a certain group of employees) could be seen to violate the *Charter* principle of equal protection.

Part 3 — Current & Future Considerations

In the 1973 report "Respect for the Privacy of Individuals," the Secretary-General of the United Nations remarked on the erosion of privacy and cautioned:

> Wholesale invasions of privacy inhibit liberty, often purposely. This is particularly true of surreptitious invasions, like electronic eavesdropping, spies, informers, entrappers, and psychological testing, the existence of which the subject is often unaware until too late. The community becomes fear-ridden, and no one can be trusted whether he be family, friend or associate; indeed, a person may be led to continual distrust of himself, as his efforts at individual self-fulfillment conflict with the norms of authority. This destruction of trust is one of the major dangers of a free society … the detailed questionnaire for employment, housing, insurance, and other matters, the hidden but suspected cameras in the washroom, the psychological tests, the lie detector and truth serum — all of these devices for ferreting out intimate and often unconscious details of our lives, produce a pervasive insecurity which suppresses individuality, discourages responsibility and encourages frightened conformity.[166]

Today, unchecked technological development is a principal threat to personal privacy. Highly sophisticated technology allows the penetration of physical barriers useful for the protection of privacy. It also renders traditional legal protections largely inadequate.[167]

Technology is also changing perceptions about privacy. Some observers think that traditional concepts of privacy are too narrow to address many concerns raised by the new employment practices. As work, for the most part, is an inherently public activity done on behalf of the employer at the place of employment, it is difficult under existing definitions for an employee to assert a right of privacy.[168]

The impact of intrusive employment practices on affected employees, and in turn, on society as a whole, have yet to be fully realized. However, as roughly half of an adult's waking hours are spent at work,[169] decisions made about workplace privacy will likely have broad and long-term social significance.

A. Existing Legal and Regulatory Framework

It has been noted that "the reports of the death of privacy in an information society are both premature and exaggerated. Developments in information technology will simply require a more skilled balancing of competing interests, such as privacy and other social values."[170] Over the past decade or so there has been a growing awareness that workplace privacy issues must be addressed and this balance equitably struck. Some limited measures have already been taken to regulate a few intrusive employment practices. Newer techniques such as computer monitoring and genetic testing have yet to have any form of government regulation.

i) Electronic Monitoring

In Ontario, disclosure of a telephone conversation by a person who is not intended to be a party to such a conversation is prohibited under the *Telephone Act*. Section 112 of the *Telephone Act* provides that:

> **112.** Every person who, having acquired knowledge of any conversation or message passing over any telephone line not addressed to or intended for such person, divulges the purport or substance of the conversation message, except when lawfully authorized or directed so to do, is guilty of an offence.

According to the findings of a case in which section 112 was considered, the purpose of the provision is to create a right of privacy with regard to telephone conversations.[171] In addition to the *Telephone Act*, the *Criminal Code* prohibits the interception of private communications, such as telephone conversations.[172] However, the *Criminal Code* provisions do not apply to the following:

- Videotape that has no sound.[173] Therefore, an employer could use soundless videotape to monitor employees, without committing an offence.
- Where there is no reasonable expectation that the communication will be private.[174] This means that if the employer warns employees ahead of time that their telephone conversations may be monitored at some time, the provisions of the *Criminal Code* may not apply.
- When one of the parties to the conversation consents to the listening in.[175] However, the constitutionality of this has been recently called into question by the Supreme Court of Canada.[176]
- To the communications services industry.[177]
- Where the interceptor has obtained judicial authorization to do so.[178]

ii) Lie Detectors

The mandatory use of lie detectors in the workplace is prohibited under the Ontario *Employment Standards Act* which states:

> **47.**–(1) An employee has a right not to take or be asked or required to take or submit to a lie detector test.
>
> (2) No person shall require, request, enable or influence directly or indirectly an employee to take or submit to a lie detector test.
>
> (3) No person shall communicate or disclose to an employer that an employee has taken a lie detector test, or communicate or disclose to an employer the results of a lie detector test.

iii) Drug Testing

There is no Ontario legislation that deals specifically with drug testing in the workplace. Although the Ontario *Human Rights Code* does not specifically address the issue of drug testing, the Commission has issued a policy on drug and alcohol testing in the workplace.[179]

The Ontario Human Rights Commission has taken the position that discrimination in employment due to a handicap includes drug or alcohol dependency. The *Code* prohibits discrimination in employment because of a handicap. Moreover, pre-employment testing for drug or alcohol dependency, or any other medical condition, has been prohibited by the Ontario Human Rights Commission.[180] Post-employment medical testing is allowed only to determine the individual's ability to perform the essential duties of a job.

Finally, the Commission has set out guidelines relating to the scope, process and procedures for testing where testing is justified. According to the guidelines, as testing for drugs may provide other information on a wide range of medical conditions, the sample should be analyzed only for the purpose for which the test is being done. The test can only be applied to determine whether a person can perform the essential duties of the job. The results of any test must be kept confidential and should not form part of the employee's personnel file.[181]

In addition, there have been a number of regulatory initiatives regarding drug testing at the federal level. In 1987, the House of Commons Standing Committee on National Health and Welfare tabled a report entitled *Booze, Pills and Dope: Reducing Substance Abuse in Canada*. The Committee opposed mass or random testing in Canada and recommended that:

- if testing must be used, it should only be conducted when grounds exist for suspecting the possible use of drugs or alcohol;
- drug screening should only be used to assist the employee in seeking appropriate treatment, and it should not be used as evidence in criminal proceedings;
- all positive test results should be confirmed by another test;
- all results should be conveyed to a licensed medical practitioner acceptable to both the employer and employee; and
- no action should be taken on the basis of positive results before the employee is given the opportunity to meet with the medical practitioner and/or to present contrary evidence.[182]

In March 1990, Transport Canada released a paper entitled *Strategy on Substance Use in Safety-Sensitive Positions in Canadian Transportation*. The strategy outlined in this paper offered a comprehensive approach to preventing substance abuse in the transportation safety environment as follows:

- under an expanded definition of what constitutes a safety-sensitive position, provide for amended or new regulations to prohibit employees in safety-sensitive positions from using, being under the influence of or impaired by a substance while on duty and from using alcohol within eight hours before work. Use of prescribed and "over-the-counter" drugs would be permitted under given conditions;

- require transportation employers to provide education to employees in safety-sensitive positions on the effects of drugs and alcohol and the requirements of federal policy and regulations intended to prevent use in the workplace;

- require that employees in safety-sensitive positions have access to an Employee Assistance Program (EAP);

- require training for supervisory personnel in the transportation safety environment on recognizing signs of substance abuse and encourage education programs in kind for all employees in safety-sensitive positions;

- require substance testing after an accident, as part of a required medical examination, as a condition of confirming a new or transferred employee in a safety-sensitive position, and "for cause" and under a program having a random element in the workplace;

- require removal of employees from safety-sensitive positions where an individual has been confirmed as having tested positively for alcohol or drugs. Reinstatement would only be possible on the recommendation of a counsellor or health professional to whom the employee was referred under the employer's EAP and;

- prevent persons having a positive test result from being confirmed in safety-sensitive positions.[183]

The federal Minister of Transportation was to pursue legislation needed to implement the strategy. However, the federal government has moved away from its initial proposal requiring mandatory random drug testing of employees. Instead, testing will only be carried out:

- after an accident or incident;

- during regular medical examinations of certain employees in safety-sensitive positions;

- during the pre-employment stage in safety-sensitive positions for both new and transferred employees; and

- during employment of employees in safety-related positions "for just cause."[184]

iv) Psychological Testing

There are no legislative restrictions on the use of psychological testing in Ontario workplaces. However, the Canadian Psychological Association has developed standards regarding the use of psychological tests. In a landmark case[185] addressing psychological testing in the workplace, a crown corporation was ordered to discontinue the use of a test for entry-level positions because the test was not validated and because it had the effect of discriminating against women. This decision strongly suggests that with the burden of proof falling to employers, they will have to defend their use of psychological testing on technical grounds (e.g., reliability and validity).[186]

v) Employment Records

Ontario's freedom of information and protection of privacy legislation[187] provides provincial and municipal employees with a right of access to their own personal information. However, there is no comparable legislation for employees in the private sector.

Under Canadian common law, private sector employers have ownership of the employment records in their possession. Unless employers agree to provide employee access to employment files, the employee has no legal right of access to his or her own records or files.[188] Even if access were provided, employers have argued for a legitimate need to exempt certain records from a general right of access, correction and amendment. Among these records might be information about individuals considered to have potential for long range advancement in the organization or company security records.[189]

Canadian court decisions have established that employers owe their employees a duty of confidentiality. When an employer requests specific information for specified purposes, or when it can be reasonably understood from the circumstances that the employer wishes certain information for specific purposes, an implied contract is created between the employer and the employee that the information will not be used for any other purposes.[190] However, Canadian courts have traditionally been reluctant to recognize a separate right to privacy.[191] Nevertheless, several Ontario courts have indicated that a cause of action for invasion of privacy does exist at common law.[192]

Most Canadian employees have no legal right to dispute the contents of personnel files, unless an employer publishes a policy or makes some other agreement permitting employees to make corrections. One exception to this rule is the right of employees in certain provinces, including Ontario, to dispute the accuracy of information provided to their employers by consumer reporting agencies.[193]

In Ontario, under the *Consumer Reporting Act*, employers who do not hire a prospective employee as a result of a negative reference from a consumer reporting agency, must inform the individual of that fact. These applicants must also be notified of the source of the negative information and the basic information obtained. The legislation also prohibits employers from seeking personal information on job applicants from consumer reporting agencies, unless the applicants have been so notified.

Under the Ontario *Human Rights Code*, employers are prohibited from collecting certain information from job applicants. Subsection 23(2) states:

> The right under section 5 to equal treatment with respect to employment is infringed where a form of application for employment is used or a written or oral inquiry is made of an applicant that directly or indirectly classifies or indicates qualifications by a prohibited ground of discrimination.

An exception to this rule is the implementation of a special program designed to relieve hardship or economic disadvantage or to assist disadvantaged persons or groups to achieve equal opportunity.[194] This exception would permit the collection of personal information for employment equity programs.

B. Assessment of Existing Framework

From the above it is apparent that government regulation of potentially intrusive employment practices is piecemeal at best, thereby providing insufficient protection against abuses. Although guidelines and court decisions are helping to further define workplace privacy rights, some privacy advocates are concerned that the pace of these developments is too slow.

In addition to legislative regulation, employment practices in unionized workplaces may be restricted by collective agreements. For example, Canadian unions have been addressing the issue of electronic monitoring since the early 1980s, focusing mostly on banning individual monitoring. A number of unions have successfully negotiated contract language limiting use of monitoring and providing a structure for reviewing complaints about surveillance.

Although labour arbitration cases have been developing a right to privacy in the workplace,[195] the collective bargaining process is viewed as not being a sufficiently far-reaching and powerful tool to regulate potentially intrusive employment practices. Based upon Statistics Canada's profile on Canada's unionized workers for 1987 (the most recent figures available at the time of writing), only 38.3 per cent of Ontario workers were unionized; slightly higher than the national total of 36.7 per cent.[196] Therefore, to leave the regulation of these practices to the collective bargaining process

means that the majority of the workforce would not be protected. After studying this issue, the Labour Canada Task Force on Micro-Electronics and Employment concluded that "collective bargaining may be a deficient instrument to provide adequately for technological change."[197]

> Even when unions are involved, technological choice, such as the decision to introduce computer equipment with monitoring capability, may be considered a management right that is not subject to bargaining, although some union contracts do require employers to bargain over change in work technology or performance standards.[198]

The call for legislative action and the cessation of certain practices has been heard for some time. Prohibition was discussed by the Ministry of Labour in its 1979 study of electronic surveillance. At that time, a number of employers indicated to the Ministry that if electronic monitoring were prohibited, they would consider increasing the numbers of supervisory personnel and/or subjecting employees to searches as they left the premises. To prohibit electronic monitoring completely, or even to restrict its use to very specific circumstances, raises the question of whether prohibition would lead to an increase in other types of monitoring.[199]

In 1982, the Labour Canada Task Force on Micro-Electronics and Employment addressed this issue and made the following recommendation:

> The Task Force regards close monitoring of work as an employment practice based on mistrust and lack of respect for basic human dignity. It is an infringement on the rights of the individual, an undesirable precedent that might be extended to other environments unless restrictions are put in place now. We strongly recommend that this practice be prohibited by law.[200]

At the beginning of 1991, the Canadian Bar Association-Ontario concluded, in its report on drug testing in the workplace, that:

> … legislation is required in order to protect the rights of unorganized employees. The common law is inadequate and our human rights commissions are already overextended. … the government should legislate effective minimum standards to protect the rights of those employees for whom mandatory drug testing is considered legitimate.[201]

More recently, in February 1992, the Canadian Civil Liberties Association (CCLA) made a submission to the Minister of Labour for Ontario regarding mandatory drug testing in the workplace. In the submission, the CCLA noted that they were helping certain affected employees process complaints under the Ontario *Human Rights Code*, but it was their view that the *Code* provides inadequate redress. Accordingly, the CCLA urged the Minister "to introduce legislation that would prohibit employers, on a universal or random basis, from requiring their employees or prospective employees to provide urine samples or other bodily fluids for drug testing."[202]

C. Future Considerations

Some observers think that the use of practices like electronic surveillance in the workplace has already achieved such an "inexorable momentum" that they may be impossible to stop. Therefore, they see the real issue as not whether a practice should be used, but rather how its use can be the least damaging for employees.[203]

If the status quo is determined to be unsatisfactory and prohibition unreasonable, there are a number of different ways to proceed to ensure that the interests of all parties involved are addressed. Three options (voluntary guidelines, legislation, and further study) are presented for the purpose of facilitating discussion.

1. Voluntary Guidelines

A number of guidelines already exist outlining the ways in which certain practices should be carried out. For example: the guidelines of the Ontario Human Rights Commission on drug and alcohol testing, the Canadian Psychological Association on the use of psychological testing, and the Human Resources Secretariat of Ontario on the treatment of personal information in government employment files, pursuant to the provisions of the *Freedom of Information and Protection of Privacy Act*. However, these are limited in their application.

The development of comprehensive voluntary guidelines could take several forms. The Ontario government could:

- encourage employers to create their own guidelines;
- develop guidelines in concert with labour and business groups, and then encourage employers to adopt them; or
- designate an agency (e.g., the Office of the Information and Privacy Commissioner, or the Human Rights Commission) to review independently developed guidelines to ensure that they met minimum standards set by the government.

Government initiative in setting guidelines or minimum standards would help ensure that the needs of all affected parties were addressed and a consensus among the stakeholders reached on a number of very difficult issues such as: who would be covered (public or private sector, or both), how the guidelines would be introduced, how they would be enforced, and whether there would be an appeal mechanism.

The advantage of this approach is that guidelines could be developed relatively expeditiously without the need for legislative or regulatory amendments. However, as compliance could not be enforced, the success of the guidelines would depend upon the voluntary co-operation of employers and employees.[204]

2. Draft Legislation

Another approach would be to regulate employment practices like employee testing, electronic monitoring, and the misuse of employment records, through legislation. As several pieces of legislation already address certain employment practices in Ontario (e.g., the *Employment Standards Act*, the *Labour Relations Act*, and the Ontario *Human Rights Code*), this option may be seen as a logical extension. As the scope of each of these pieces of legislation is different, the advantages and disadvantages of each must be carefully examined in order to determine which statute(s) could be amended.

How legislative regulation is introduced could vary:

- different practices could be addressed separately under different statutes, or dealt with in a single piece of legislation;
- existing statute(s) could be amended or new legislation introduced.

In 1980, 1981 and 1982, identical Bills about electronic surveillance (Bills 105, 32 and 78, respectively) were introduced by a Private Member of the Ontario Legislature. In these Bills it was proposed that the *Employment Standards Act* be amended as follows:

> **15a.** No employer shall install or operate an electronic surveillance device or system in a place of employment to record or monitor the work and other activities of his employees unless the installation and operation of such device or system is reasonably necessary, the proof of which lies upon the employer, for the protection of the health and safety of the employees. (Bill 78, 1982)

Although the Bills did not receive second reading, they suggest a possible method of addressing electronic surveillance in Ontario.

In 1984, a Bill was introduced in the Ontario Legislature to give employees statutory rights regarding employment record confidentiality through an amendment to the *Employment Standards Act*. Again this Bill did not pass and become law, but it is an example of the type of statutory provision that could be adopted in Ontario. Subsection 11(a) of the Bill stated:

(1) An employee has a right to see and shall on request be given access to the employer's personnel records relating to the employee.

(2) An employee has a right to have errors or omissions in the employer's personnel records relating to the employee corrected.

(3) An employer who refuses to make a correction requested by an employee under subsection (2) shall,

(a) notify the employee that the employer refuses to make the correction as requested; and

(b) note the request and response in the personnel record relating to the employee.

(4) An employee who is dissatisfied with an employer's refusal to make a correction to a personnel record relating to the employee may request that an employment standards officer investigate and seek to conciliate the matter.[205]

Due to the limitations of the existing legislation (e.g., some are only applicable to the public sector, and some do not have regulatory agencies with order-making powers), the most appropriate option may be to draft legislation to regulate this new generation of employment practices.

3. Further Study

As limited research has been conducted on the extent and impact of these new workplace practices in Ontario, it may be premature to attempt any form of regulation at this time. Accordingly, further study of these issues in the form of a government initiative with consultation with business, labour and advocacy groups, is another option.

Further study would enable the government to properly determine the extent of these practices in Ontario and how they are affecting the workplace. After such a study, the government would be in an excellent position to determine what, if any, regulatory scheme would be the most appropriate.

Notes

1. *R.* v. *Dyment* [1988] 2 S.C.R. 417 at 427–428, 55 D.L.R. (4th) 503 at 513, 89 N.R. 249 at 260.

2. Gary T. Marx and Sanford Sherizen, "Monitoring on the Job: How to Protect Privacy as Well as Property," *Technology Review*, Vol. 89, No. 8, Nov/Dec 1986, p. 65.

3. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol. IV, No. 5, December 1890, p. 193.

4. Carol C. Gould, "Network Ethics: Access, Control, and the Informed Community," *The Information Web: Ethical and Social Implications of Computer Networking*, Edited by Carol C. Gould (San Francisco: Westview Press, 1989), p. 23.

5. Jane Ford, "The Right to Privacy in Employment: A Management Perspective," *Labour Arbitration Yearbook 1991*, Edited by William Kaplan, Jeffrey Sack, and Morley Gunderson, (Toronto: Butterworths-Lancaster House, 1991), p. 96.

6. Commission on Freedom of Information and Individual Privacy, *Public Government for Private People*, Vol. 3, (Toronto: Queen's Printer of Ontario, 1980), p. 495.

7. These three types of privacy were identified and defined by the federal Canadian Task Force on Privacy and Computers as follows:

   Territorial Privacy

   Claims to privacy advanced in a territorial or spatial sense are related historically, legally and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquillity is advanced and recognized. A man's home is his castle. At home he may not be disturbed by trespassers, noxious odours, loud noises, or peeping Toms. No one may enter without his permission, except by lawful warrant.

   Privacy of Person

   In a second sense, a claim to the privacy of one's person is protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person. This notion, like the territorial one, is spatial in the sense that the physical personal is deemed to be surrounded by a bubble or aura protecting him from physical harassment. But, unlike physical property, this "personal space" is not bounded by real walls and fences, but by legal norms and social values. Furthermore, this sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person.

Our persons are protected not so much against the physical search … as against the indignity of the search, its invasion of the person in a moral sense.

Privacy in the Information Context

The third category of claims to privacy … is based essentially on a notion of the dignity and integrity of the individual, and on their relationship to information about him.

This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. And this is so whether or not the information is subsequently communicated accurately, and whether or not it is potentially damaging to his reputation, his pocket-book, or his prospects; the context is of course the controlling factor in determining whether or not particular information will be damaging. Competing social values may require that an individual disclose certain information to particular authorities under certain circumstances (e.g., census information). He may decide to make it available in order to obtain certain benefits (e.g., credit information or information imparted to his lawyer to win a lawsuit or to his confessor to win salvation). He may also share quite willingly with his intimates. Nevertheless, he has a basic and continuing interest in what happens to this information, and in controlling access to it.

Canada, Department of Communications and Department of Justice, *Privacy and Computers* (Ottawa: Information Canada, 1972), pp. 13–14, as cited in Commission on Freedom of Information and Individual Privacy, *Public Government for Private People*, Vol. 3, pp. 499–500.

8. United States Congress, Office of Technology Assessment, *The Electronic Supervisor: New Technology, New Tensions* (Washington, D.C.: United States Government Printing Office, September 1987), p. 19.

9. Alan F. Westin, as quoted in John Hoer with Katherine M. Hafner, Gail DeGeorge, Anne R. Field and Laura Zinn, "Privacy," *Business Week*, March 28, 1988, p. 62.

10. Hoer, *et al.*, "Privacy," p. 61.

11. Beverly Potter and Sebastian Orfali, *Drug Testing at Work: A Guide for Employers and Employees* (Berkeley: Ronin Publishing Inc., 1990), p. 1.

12. Marx and Sherizen, "Monitoring on the Job," p. 64.

13. The Information and Privacy Commissioner/Ontario addressed the issue of AIDS in two reports: "HIV/AIDS in the Workplace" and "HIV/AIDS: A Need for Privacy."

14. Leslie Papp, "Working Under the Electronic Eye," *Toronto Star*, July 27, 1991, p. D1.

15. Marx and Sherizen, "Monitoring on the Job," p. 65.

16. Office of Technology Assessment, *Electronic Supervisor*, p. 5.

17. Oscar H. Gandy, Jr., "The Surveillance Society: Information Technology and Bureaucratic Social Control," *Journal of Communication*, Vol. 39, No. 3, Summer 1989, pp. 63–64.

18. Ministry of Labour Research Branch, *Electronic Surveillance: A Discussion Paper*, No. 21 (Toronto: Ontario Ministry of Labour, 1979), p. 3.

19. Geoff Bickerton and Jane Stinson, "Working in 1984," *Rights and Freedoms*, No. 50, January–February 1984, p. 8.

20. Ibid.

21. Ann Gibbon, "An Eye from Afar," *Globe and Mail*, August 23, 1990, p. B5.

22. Office of Technology Assessment, *Electronic Supervisor*, p. 105.

23. Privacy Committee and Labour Council of New South Wales, "Guidelines for Telephone Usage Monitoring Systems/Telephone Information and Management Systems," *Information Bulletin* (Sydney, November 14, 1983), p. 1.

24. Office of Technology Assessment, *Electronic Supervisor*, p. 35.

25. Andrew Clement, "Electronic Management: The New Technology of Workplace Surveillance," *Proceedings of CIPS Session 84*, Calgary, Alberta, May 9–11, 1984, pp. 2–3.

26. Office of Technology Assessment, *Electronic Supervisor*, p. 30.

27. Paul B. Carroll, "Sounding off on Big Blue's Democracy Wall," *The Globe and Mail*, August 10, 1991, p. B1.

28. Rebecca A. Grant, "Computerized Performance Monitoring and Control Systems: Impact on Canadian Service Sector Workers," Ph.D. Thesis for the University of Western Ontario, September 1988.

29. Ibid., pp. 5–6.

30. Office of Technology Assessment, *Electronic Supervisor*, p. 28.

31. Willis H. Ware, *Emerging Privacy Issues* (Santa Monica: The Rand Corporation, October 1985), pp. 4–5.

32. Marx and Sherizen, "Monitoring on the Job," p. 67.

33. Rachel Blau, "Big Brother is Not Just Watching…," *Labour Occupational Health Program Monitor*, Vol. 16, No. 2, Summer 1988, p. 9.

34. "Biometric Access Control Systems: Technology Overview," *Datapro Report on Information Security*, January 1990, pp. 321–322.

35. Ian A. Miners, Nick Nykodym, and Diane M. Samerdyke-Traband, "Put Drug Detection to the Test," as reprinted in *Employee Testing: The Complete Resource Guide* (Washington, D.C.: The Bureau of National Affairs, Inc., 1988), p. III–54.

36. Ibid.

37. *Privacy Times*, Vol. 11, No. 9, May 23, 1991, p. 8.

38. Ira Michael Shepard, Robert Duston and Karen S. Russell, *Workplace Privacy: Employee Testing, Surveillance, Wrongful Discharge, and Other Areas of Vulnerability* (Washington, D.C.: The Bureau of National Affairs, Inc., 1989), p. 192.

39. United States Congress, Office of Technology Assessment, *Genetic Monitoring and Screening in the Workplace* (Washington, D.C.: United States Government Printing Office, October 1990), p. 251.

40. *Privacy Times*, January 15, 1992, p. 3.

41. Shepard, Duston and Russell, *Workplace Privacy*, p. 92.

42. Ibid.

43. Ibid., p. 147.

44. Ibid.

45. A. Anastasi, *Psychological Testing and Measurement* (New York: MacMillan Publishing Co., 1982), p. 15.

46. C.H. Stone and F.L. Ruch, "Selecting, Interviewing, and Testing," *ASPA Handbook of Personnel and Industrial Relations*, Edited by D. Yoder and H.G. Herman (Washington, D.C.: The Bureau of National Affairs, 1979), p. 4–140.

47. Rosemary Amelia Venne, *Psychological Testing in Personnel Selection* (Kingston, Ontario: School of Industrial Relations Research Series, No. 8, Queen's University, 1987), p. 14.

48. Shepard, Duston and Russell, *Workplace Privacy*, pp. 152–153.

49. James C. Crumbaugh, "Graphoanalytic Cues," as reprinted in *Employee Testing: The Complete Resource Guide*, pp. VI–52 & VI–53.

50. Shepard, Duston and Russell, *Workplace Privacy*, p. 295.

51. United States Congress, Office of Technology Assessment, *Automation of America's Offices, 1985–2000* (Washington, D.C.: National Technical Information Service, 1985), p. 72.

52. Science Council of Canada, *A Workshop on Information Technologies and Personal Privacy in Canada* (Ottawa: Minister of Supply and Services, 1985), p. 20.

53. Tim Beardsley, "Electronic Taskmasters: Does Monitoring Degrade the Quality of Working Life?" *Scientific American*, Vol. 257, No. 6, December 1987, p. 36.

54. Carl B. Jackson, "Need for Security," *Datapro Reports on Information Security*, October 1990, p. 7.

55. Peter A. Susser, "Electronic Monitoring in the Private Sector: How Closely Should Employers Supervise Their Workers?" *Employee Relations Law Journal*, Vol. 13, Spring 1988, p. 576.

56. Jackson, "Need for Security," p. 7.

57. Potter and Orfali, *Drug Testing at Work*, p. 24.

58. August Bequai, "Drug Testing: Security, Privacy, and the Law," *Datapro Reports on Information Security*, November 1987, p. 1.

59. Potter and Orfali, *Drug Testing at Work*, p. 24.

60. Ibid., p. 25.

61. Royal Canadian Mounted Police, *Drugs in the Workplace* (Ottawa: Minister of Supply and Services Canada, 1988), p. 9.

62. Projection of the Addiction Research Foundation based on $42 billion per year cost estimated by the White House Office of Drug Abuse. In *Preventing drug abuse in the workplace*, Edited by J.R. Vicary and H. Resnick (United States Department of Health and Human Services, No. ADH 82–1220), as cited by Royal Canadian Mounted Police, *Drugs in the Workplace*, p. 9.

63. Royal Canadian Mounted Police, *Drugs in the Workplace*, p. 9.

64. Bertrand Marotte, "War Against Drug Testing Escalates," *The Montreal Gazette*, October 10, 1991, p. C2.

65. James E. Dorsey and Susan D. Charlton, "Alcoholism, Drug Dependency and the Workplace: Problems and Responses," *Labour Arbitration Yearbook 1991*, p. 72.

66. President of Reid Psychological Systems citing a U.S. Chamber of Commerce statistic in "Psychologists Disagree About Value of Honesty Testing of Employees," as reprinted in *Employee Testing: The Complete Resource Guide*, p. II–1.

67. Chris Chenoweth, "Stealing from the company: The Rising Toll," *Toronto Star*, July 17, 1983, p. H3.

68. John Southerst, "Managerial Vigilance Still Best Way to Put an End to Employee Crime," *Financial Post*, May 25, 1987, p. 23.

69. Martin Dewey, "Time Waster on the Job: Thief or Free-wheeler?" *The Globe and Mail*, April 27, 1981, p. B2.

70. Curt Rush, "Thieves are at Work — Stealing Time," *Toronto Star*, July 1, 1984, p. H1.

71. Shepard, Duston and Russell, *Workplace Privacy*, p. 152.

72. Ministry of Labour, *Electronic Surveillance*, p. 5.

73. Jackson, "The Need for Security," p. 6.

74. Christine Casatelli, "Setting Ground Rules for Privacy," *Computerworld*, March 18, 1991, p. 50.

75. Sandra T. Sampson, "Privacy: The Invasion of the E-Mail Snatchers," *Datapro InfoSecurity*, Vol. 7, No. 4, April 1991, p.1.

76. "Rights Agency Probes Firm's Drug Testing," *Toronto Star*, January 9, 1992.

77. United States Congress, Office of Technology Assessment, *The Role of Genetic Testing in the Prevention of Occupational Disease* (Washington, D.C.: United States Government Printing Office, 1983), p. 5.

78. Jane Ford, "The Right to Privacy in Employment: A Management Perspective," *Labour Arbitration Yearbook 1991*, Vol. 1, p. 102.

79. Zachary Schiller, Walecia Konrad with Stephanie Anderson Forest, "If You Light Up on Sunday, Don't Come in on Monday," *Business Week*, August 26, 1991, p. 68.

80. Ibid., p. 69.

81. John G. Fleming, *The Law of Torts* (Sydney, Australia: The Law Book Company, 1987), pp. 359–360.

82. Marx and Sherizen, "Monitoring on the Job," p. 71.

83. Susser, "Electronic Monitoring in the Private Sector," pp. 578–579.

84. Ministry of Labour, *Electronic Surveillance*, p. 1.

85. Ibid., p. 14.

86. Grant, "Computerized Performance Monitoring and Control Systems," p. 9.

87. Rebecca Grant and Christopher Higgins, "Monitoring Service Workers via Computer: The Effect on Employees, Productivity, and Service," *National Productivity Review*, Vol. 8, No. 2, Spring 1989, p. 102.

88. Marx and Sherizen, "Monitoring on the Job," p. 67.

89. Science Council of Canada, *A Workshop on Information Technologies and Personal Privacy in Canada* (Ottawa: Minister of Supply and Services, 1985), p. 21.

90. Lisa Gallatin, *Electronic Monitoring in the Workplace: Supervision or Surveillance?* (Boston: Massachusetts Coalition on New Office Technology, February 28, 1989), p. 20.

91. Marx and Sherizen, "Monitoring on the Job," pp. 67 & 70.

92. Michael Lynk, "Chemical McCarthyism: Workplace Mandatory Drug Testing" (April 1988), *Canadian Transport*, p. 4, as cited by Paul J.J. Cavalluzzo and Karen Schucher, *Drug Testing in the Workplace*, Canadian Bar Association-Ontario, January 17, 1991, p. 2.

93. Donn B. Parker, "Information Security Myths Explained," *Datapro Reports on Information Security*, June 1990, p. 2.

94. Minister of Labour, *Electronic Surveillance*, pp. 8–9.

95. Office of Technology Assessment, *Electronic Supervisor*, p. 76.

96. Ibid., p. 69.

97. James E. Dorsey and Susan D. Charlton, "Alcoholism, Drug Dependency and the Workplace: Problems and Responses," *Labour Arbitration Yearbook 1991*, Vol. 1, p. 74.

98. Hoerr *et al.*, "Privacy," p. 68.

99. *Websters Third New International Dictionary*, Philip Babcock Gove, Editor in Chief (Springfield, Massachusetts: Merriam-Webster, Inc., 1986) p. 148.

100. Office of Technology Assessment, *The Role of Genetic Testing*, p. 142.

101. Privacy Commissioner of Canada, *Drug Testing and Privacy* (Ottawa: Minister of Supply and Services Canada, 1990), p. 20.

102. Office of Technology Assessment, *Role of Genetic Testing*, p. 142.

103. Marx and Sherizen, "Monitoring on the Job," pp. 65–66.

104. Office of Technology Assessment, *Electronic Supervisor*, p. 8.

105. *Black's Law Dictionary* (St. Pauls: West Publishing Co., 1990), p. 305.

106. Robert Ellis Smith, *Privacy — How to Protect What's Left of It*, (n.p., 1979), p. 68.

107. *Black's Law Dictionary* (St. Pauls: West Publishing Co., 1990), p. 779.

108. FMC Corp. v. U.A.W. (46, Lab. Arb. 335 [1966] or 66–1 CCH Lab. Arb. Awards, para 8287 [1966]), as cited on Ministry of Labour, *Electronic Surveillance*, p. 12.

109. Ministry of Labour, *Electronic Surveillance*, p. 12.

110. Standing Committee on Justice and Solicitor General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (Ottawa: Queen's Printer, March 1987), p. 71.

111. Office of Technology Assessment, *Electronic Supervisor*, p. 11.

112. A toilet has been recently invented that collects and transmits measurements of blood pressure, pulse rate, body temperature and weight, and provides a urine analysis within five minutes of contact with the toilet seat. The accompanying processor can store the information for up to 130 days, print it out or transfer it to a personal computer. As noted in *Privacy Times*, March 14, 1990, p. 8.

113. Privacy Commissioner of Canada, *Drug Testing and Privacy*, p. 18.

114. *R. v. Dyment* [1988] 2 S.C.R. 417 at 431–32, as cited in Privacy Commissioner of Canada, *Drug Testing and Privacy*, p. 18.

115. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 7.

116. Deborah G. Johnson, *Computer Ethics*, (Englewood Cliffs, NJ: Prentice-Hall, 1985), p. 66, as cited in James H. Moor, "How to Invade and Protect Privacy with Computers," *The Information Web: Ethical and Social Implications of Computer Networking*, pp. 60–61.

117. Science Council of Canada, *Workshop*, p. 9.

118. Gary T. Marx, "Privacy and Technology," *The World and I*, Vol. 5, No. 9, September 1990, p. 534.

119. Kurt H. Decker, *A Manager's Guide to Employee Privacy Laws, Policies, and Procedures* (New York: John Wiley & Sons, Inc., 1989), p. 148.

120. Shepard, Duston and Russell, *Workplace Privacy*, p. 296.

121. David F. Linowes, "Employee Rights to Privacy and Access to Personnel: A New Look," *Employee Relations Law Journal*, Vol. 4, No. 1, Summer 1978, p. 35.

122. Arthur Miller, "Statement to Sub-Committee of U.S. Senate on Administrative Practice and Procedure," (Washington, D.C.: March 14, 1967) as cited in Arthur J. Cordell, *The Uneasy Eighties: The Transition to an Information Society* (Ottawa: Ministry of Supply and Services Canada, 1985), p. 74.

123. "Electronic Surveillance and Control of the Workplace," Speech by Christine Micklewright, Vice General Chairperson, Brotherhood of Railway and Airline Clerks, to the Science Council of Canada Workshop on Information Technologies and Personal Privacy, Ottawa, 1984, pp. 1–2.

124. Ford, "The Right to Privacy in Employment," p. 99.

125. David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (Chicago: University of Illinois Press, 1989), p. 15.

126. Miners, Nykodym and Samerdyke-Traband, "Put Drug Detection to the Test," *Employee Testing: The Complete Resource Guide*, p. III–55.

127. Cathie Shattuck, "The Tort of Negligent Hiring," p. 3.

128. Miners, Nykodym and Samerdyke-Traband, "Put Drug Detection to the Test," *Employee Testing: The Complete Resource Guide*, p. III–56.

129. Privacy Committee of New South Wales, *Electronic Vehicle Tracking*, Issues Paper No. 62 (Sydney: Privacy Committee of New South Wales, August 1990), p. 9.

130. David F. Linowes, *Privacy in America*, p. 15.

131. Canadian Bar Association-Ontario, *Report on Mandatory Drug Testing*, July 1987, p. 14.

132. David Linowes, *Privacy in America*, p. 15.

133. Dr. Robert Pokorski, "New Technologies in Underwriting: Genetic Testing," *Canadian Insurance/Agent & Broker*, January 1992, p. 28.

134. Ibid.

135. Office of Technology Assessment, *Genetic Monitoring and Screening*, p. 11.

136. Ibid., p. 71.

137. Pokorski, "New Technologies in Underwriting: Genetic Testing," p. 30.

138. Shepard, Duston and Russel, *Workplace Privacy*, p. 93.

139. *Privacy Times*, Vol. 10, No. 18, September 28, 1990, p. 6.

140. D.J. Yoder and P.D. Staudohar, "Testing and EEO: Getting Down to Cases," *Personnel Administrator* Vol. 29, No. 2, 1984, p. 70.

141. Executive Director of the Foundation on Economic Trends, as cited by William Pat Patterson, "Genetic Screening: How Much Should we Test Employees?" *Employee Testing: The Complete Resource Guide*, p. V–12.

142. Office of Technology Assessment, *Role of Genetic Testing*, p. 141.

143. Results from survey conducted by Clinic for Inherited Diseases at Harvard Medical School's Deaconess Hospital, as cited in Simon L. Garfinkel, "Insurers Take an Interest in Genetic Findings," *Privacy Journal*, April 1991, Vol. XVII, No. 6, p. 5.

144. Alan F. Westin, Columbia University professor, as cited in Schiller, Konrad and Anderson Forest, "Light up on Sunday…" p. 72.

145. Office of Technology Assessment, *Role of Genetic Testing*, p. 144.

146. Marx and Sherizen, "Monitoring on the Job," p. 67.

147. 9 to 5, *Stories of Mistrust and Manipulation: The Electronic Monitoring of the American Workforce* (Cleveland: Working Women Education Fund, February 1990), p. 5.

148. Shepard, Duston and Russell, *Workplace Privacy*, p. 296.

149. Kurt H. Decker, *A Manager's Guide to Employee Privacy Laws, Policies, and Procedures* (New York: John Wiley & Sons, Inc., 1989), p. 136.

150. *Privacy Times*, Vol. 10, No. 18, September 28, 1990, p. 5.

151. "Surveillance and Individual Privacy," *U.N. Chronicle*, April 1983, p. 27.

152. Marx and Sherizen, "Monitoring on the Job," pp. 65–66.

153. Clement, "Electronic Management," p. 2.

154. David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: The University of North Carolina Press, 1989), p. 3.

155. Marshall McLuhan and Quentin Fiore, *War and Peace in the Global Village* (New York: McGraw-Hill, 1968) as cited in Science Council of Canada, *Workshop*, p. 9.

156. Marx and Sherizen, "Monitoring on the Job," p. 70.

157. Ibid., p. 71.

158. Labour Canada Task Force on Micro-Electronics and Employment, *In the Chips: Opportunities, People, Partnerships* (Ottawa: Minister of Supply and Services Canada, 1982), p. 5.

159. *Constitution Act, 1982* [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B]. as amended.

160. Canadian Bar Association-Ontario, *Report on Mandatory Drug Testing*, p. 26.

161. Privacy Committee of New South Wales, *The Privacy Bulletin*, Vol. 4, No. 1, June 1988, p. 1.

162. *Re Dion and the Queen* (1986), 30 C.C.C. (3d) 108 (Que. S.C.) and *Jackson* v. *Joyceville Penitentiary* (1990), 55 C.C.C. (3d) 50.

163. Cavalluzzo and Schucher, *Drug Testing in the Workplace*, p. 17.

164. *Jackson* v. *Joyceville Penitentiary* (1990), 55 C.C.C. (3d) 50.

165. *Re Dion and the Queen* (1986), 30 C.C.C. (3d) 108 (Que. S.C.) as cited in Canadian Bar Association-Ontario, *Report on Mandatory Drug Testing*, p. 25–26.

166. UN Doc E/CN. 4/1116 as cited in Freedman, *The Right to Privacy*, p. 122.

167. Law Reform Commission of Australia, *Privacy*, Report No. 22, Vol.1 (Canberra: Australian Government Publishing Service, 1983) p. 40.

168. Office of Technology Assessment, *Electronic Supervisor*, pp. 89–90.

169. Labour Canada Task Force, *In the Chips*, p. 6.

170. Professor David Flaherty's concluding remarks, Science Council of Canada, *Workshop*, p. 47.

171. *R. v. Chapman and Grange* [1937] 2 O.R. 290, 34 D.L.R. 510 at 517, affg. 20 C.R.N.S. at 142 (Ont. Co. Ct).

172. *Criminal Code*, R.S.C. 1985, Chap. C–46, ss. 183–196.

173. *R. v. Biasi et al. (No. 3)* (1981), 66 C.C.C. (2d) 566 (B.C.S.C.); *R. v. Wong et al.* (1987), 34 C.C.C. (3d) 51 (Ont. C.A.) at 60, aff'd (1990) 120 N.R. 34 (S.C.C.) at 55–56. See also "How to deal with electronic surveillance in the workplace," *Focus on Canadian Employment and Equality Rights* Vol. 1, No. 17, p. 131.

174. The *Criminal Code* provisions apply only to private communications. "Private communication" is defined in section 183 as follows:

> … any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.

175. *Criminal Code*, R.S.C. 1985, Chap. C–46, s. 184(2)(a).

176. *R. v. Duarte* [1990] 1 S.C.R. 30.

177. *Criminal Code*, R.S.C. 1985, Chap. C–46, s. 184(2)(c).

178. *Criminal Code*, R.S.C. 1985, Chap. C–46, s. 184(2)(b).

179. Ontario Human Rights Commission, *Policy Statement on Drugs and Alcohol Testing*, November 1990.

180. Ontario Human Rights Commission, *Policy on Employee-related Medical Information*, April 1990.

181. Cavalluzzo and Schucher, *Drug Testing in the Workplace*, pp. 10–13.

182. Jean-Daniel Belanger, *Drug Testing: Legal Implications*, Current Issue Review, 90–1E, Library of Parliament, Research Branch, April 20, 1990, p. 13.

183. Transport Canada, *Strategy on Substance Abuse in Safety-sensitive Positions in Canadian Transportation* (Ottawa: March 1990), pp. 10–11.

184. Transport Canada, *Substance Use in Safety-Sensitive Positions in Canadian Transportation: Government Response to the Third Report of the Standing Committee on Transport*, November 1990.

185. *Action Travail des Femmes* v. *Canadian National* (1984) 5 C.H.R.R. D/2327 (Canadian Human Rights Tribunal).

186. Steven F. Cronshaw, "The Status of Employment Testing in Canada: A Review and Evaluation of Theory and Professional Practice," Vol. 27, No. 2, 1986, p. 186.

187. *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, Chap. F. 31, and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, Chap. M. 56.

188. Howard A. Levitt, "Employee Privacy: Part II, Practical Applications in the Workplace," *The Employment Law Report*, Vol. 2, No. 9, September 1981, p. 68.

189. Sarah P. Collins, *The Privacy Protection Study Commission: Background and Recommendations* (Washington, D.C.: Library of Congress, 1979), p. CRS–43.

190. Levitt, "Employee Privacy," p. 69.

191. Alan Linden, *Canadian Tort Law* (Toronto: Butterworths, 1987), p. 52.

192. See *Saccone* v. *Orr* (1981), 19 C.C.L.T. 37, (Ont. County Ct.), *Capan* v. *Capan* (1980), 14 C.C.L.T. 191, (Ont. Supreme Ct.), *P.F.* v. *Ontario et al.* (1989), 47 C.C.L.T. 231, (Ont. District Ct.), *Roth v. Roth* (1991) 4 O.R. (3d) 740 (Ont. Court, General Division).

193. Levitt, "Employee Privacy," p. 68.

194. *Human Rights Code*, R.S.O. 1990, Chap. H. 19, section 14.

195. See Donald Brown and David Beatty, *Canadian Labour Arbitration* (Toronto: Canada Law Book, 1981), 7:3625 ("Personal Privacy").

196. Statistics Canada, *Canada's Unionized Workers: A Profile of Their 1987 Labour Market Experience* (Ottawa: Minister of Supply and Services Canada, 1991).

197. Labour Canada Task Force, *In the Chips*, p. 11.

198. Office of Technology Assessment, *Electronic Supervisor*, p. 9.

199. Ministry of Labour, *Electronic Surveillance*, pp. 7–8.

200. Labour Canada Task Force, *In the Chips*, p. 56.

201. Cavalluzzo and Schucher, *Drug Testing in the Workplace*, pp. 29–30.

202. Canadian Civil Liberties Association, *Mandatory Drug Testing in the Workplace*, Submission to The Honourable Bob Mackenzie, Minister of Labour for Ontario, February 21, 1992, pp. 5–6.

203. Science Council of Canada, *Workshop*, p. 20.

204. Ministry of Labour, *Electronic Surveillance*, p. 25.

205. Bill 20, *An Act to Amend the Employment Standards Amendment Act*, 4th Sess. 32d Leg. Ont., 1984.

Bibliography

Adler, Philip Jr., Parsons, Charles K., Zolke, Scott B. "Employee Privacy: Legal and Research Developments and Implications for Personnel Administration." *Sloan Management Review*, Vol. 26, No. 2, Winter 1985.

Anastasi, A. *Psychological Testing and Measurement*. New York: MacMillan Publishing Co., 1982.

ASPA Handbook of Personnel and Industrial Relations, D. Yoder and H.G. Herman Editors, Washington D.C.: Bureau of National Affairs, 1979.

Barba, Connie. "That's No 'Beep', That's My Boss: Congress Seeks to Disconnect the Secrecy of Telephone Monitoring in the Workplace." *John Marshall Law Review*, Vol. 21, Summer 1988, pp. 881–902.

Bawden, Brian R. "Rights of Anonymity and Right of Solitude: Ethical Information Management in the Private Sector." *Canadian Public Administration*, Vol. 34, No. 1, Spring 1991, pp. 101–110.

Beardsley, Tim. "Electronic Taskmasters: Does Monitoring Degrade the Quality of Working Life?" *Scientific American*, Vol. 257, No. 6, December 1987, pp. 32, 36–37.

Belanger, Jean-Daniel. *Drug Testing: Legal Implications*, Current Issue Review, 90–1E, Library of Parliament, Research Branch. Ottawa: Library of Parliament, April 1990.

Berenbeim, Ronald E. *Employee Privacy*. Research Report No. 945. New York: The Conference Board, Inc., 1990.

Bickerton, Geoff, and Stinson, Jane. "Working in 1984." *Rights and Freedoms*, No. 50, January–February 1984, pp. 8–13.

Blau, Rachel. "Big Brother is Not Just Watching..." *Labour Occupational Health Program Monitor*, Vol. 16, No. 2, Summer 1988, pp. 8–12.

Bota, Anthony N. *Employment Related Drug Testing: The Legal Implications for Employers*. Kingston: Industrial Relations Centre, Queen's University, 1989.

Brief to the Standing Committee on Transport Re: Strategy on Substance Use in Safety Sensitive Positions in Canadian Transport. CAW Canada, May 1990.

Bureau of National Affairs. *Employee Testing: The Complete Resource Guide*. Washington, D.C.: The Bureau of National Affairs, Inc., 1988.

Canadian Bar Association-Ontario. *Report on Mandatory Drug Testing*. July 1987.

Canadian Centre for Occupational Health and Safety. *Workshop on Drug Testing in the Workplace*. P87–11E Hamilton, Ontario: 1987.

Canadian Civil Liberties Association. *Mandatory Drug Testing in the Workplace*, Submission to the Honourable Bob Mackenzie, Minister of Labour for Ontario, February 21, 1992.

Carroll, Paul B. "Sounding Off on Big Blue's Democracy Wall." *Globe and Mail*, August 10, 1991, pp. B1 & B2.

Casatelli, Christine. "Setting Ground Rules for Privacy." *Computerworld*, March 18, 1991, pp. 47 & 50.

Cavalluzzo, Paul J.J. and Schucher, Karen. *Drug Testing in the Workplace*. Canadian Bar Association-Ontario, January 17, 1991.

Chapnik, Sandra. "Mandatory Drug Testing in the Workplace." *Administrative Law Journal*, Vol. 5, No. 4, 1990, pp. 102–110.

Chenoweth, Chris. "Stealing from the Company: The Rising Toll." *Toronto Star*, July 17, 1983, p. H3.

Clement, Andrew. "Electronic Management: The New Technology of Workplace Surveillance.: *Proceedings of CIPS Session 84*, Calgary, Alberta, May 9–11, 1984.

Clement, Andrew; and McDermott, Patricia. "Electronic Monitoring: Workers Reactions and Design Alternatives." *Information System, Work and Organization Design*, Proceedings of the IFIP TC9/WG9.1 Working Conference on Information System, Work and Organization Design, Berlin, July 10–13, 1989.

Cohen, Stanley A. *Invasion of Privacy: Police and Electronic Surveillance in Canada*. Toronto: The Carswell Company Limited, 1983.

Collins, Sarah P. *The Privacy Protection Study Commission: Background and Recommendations* Washington, D.C., Library of Congress, 1979.

Commission on Freedom of Information and Individual Privacy. *Public Government for Private People*. Vol. 3. Toronto: Queen's Printer of Ontario, 1980.

Cordell, Arthur J. *The Uneasy Eighties: The Transition to an Information Society*. Ottawa: Ministry of Supply and Services Canada, 1985.

Cronshaw, Steven F., "The Status of Employment Testing in Canada: A Review and Evaluation of Theory and Professional Practice." *Canadian Psychology*, Vol. 27, No. 2, 1986, pp. 183–195.

Danann, Sharon. "Cracking the Electronic Whip." *Harper's*, Vol. 281, No. 1683, August 1990, pp. 58–59.

Datapro Research Group, *Datapro Reports on Information Security*. Delcan, N.J.: McGraw-Hill Incorporated, 1991.

Decker, Kurt H. *A Manager's Guide to Employee Privacy Laws, Policies, and Procedures* New York, John Wiley & Sons, Inc., 1989.

Dewey, Martin. "Time Waster on the Job: Thief or Free-wheeler?" *Globe and Mail*, April 27, 1981, p. B2.

Dunsmore, R. Ross. "How to Reduce the High Cost of Employee Absenteeism." *Financial Times*, May 4, 1987, p. 41.

"Electronic Surveillance and Control of the Workplace." Speech by Christine Micklewright, Vice General Chairperson, Brotherhood of Railway and Airline Clerks, to the Science Council of Canada Workshop on Information Technologies and Personal Privacy, Ottawa, 1984.

Federal Government Information Technology: Electronic Surveillance and Civil Liberties. Washington, D.C.: United States Congress, Office of Technology Assessment, October 1985.

Feingold, Barry C. "Rising Costs of Substance Abuse Demand Effective Corporate Policies." *Occupational Health and Safety*, Vol. 58, No. 10, September 1989, pp. 56 & 59.

Flaherty, David H. *Protecting Privacy in Surveillance Societies*. Chapel Hill: The University of North Carolina Press, 1989.

Flaherty, David. "The Emergence of Surveillance Societies in the Western World: Toward the Year 2000." *Government Information Quarterly*. 1988, 5 (4), 377–387.

Fleming, John G. *The Law of Torts*. Sydney, Australia: The Law Book Company, 1987.

Ford, Jane A. *Drug Testing in the Workplace*. Canadian Bar Association – Ontario, November 25, 1988.

Freedman, Warren. *The Right to Privacy in the Computer Age*. New York: Quorum Books, 1987.

Gallatin, Lisa. *Electronic Monitoring in the Workplace: Supervision or Surveillance?* Boston: Massachusetts Coalition on New Office Technology, February 28, 1989.

Gandy, Oscar H. "The Surveillance Society: Information Technology and Bureaucratic Social Control." *Journal of Communication*, Vol. 39, No. 3, Summer 1989, pp. 61–76.

Garson, Barbara. *The Electronic Sweatshop*. Toronto: Simon and Schuster, 1988.

Gates, Bruce. "Monitoring Systems to Help Firms Control Phone Costs." *Financial Post*, February 2, 1985, p. S2.

Gibbon, Ann. "An Eye from Afar." *Globe and Mail*, August 23, 1990, p. B5.

Grace, John. "The Ethics of Information Management." *Canadian Public Administration*, Vol. 34, No. 1, Spring 1991, pp. 95–100.

Grant, Rebecca A. "Computerized Performance Monitoring and Control Systems: Impact on Canadian Service Sector Workers" Ph.D. Thesis for the University of Western Ontario, September 1988.

Grant, Rebecca; and Higgins, Christopher. "Monitoring Service Workers via Computer: The Effect on Employees, Productivity, and Service." *National Productivity Review*, Vol. 8, No. 2, Spring 1989, pp. 101–112.

Gross, Hyman. "The Concept of Privacy." *New York University Law Review*, Vol. 42, 1967, pp. 34–54.

Hartigan, John A. and Wigdor, Alexandra K. (Eds.) *Fairness In Employment Testing: Validity, Generalization, Minority Issues, and the General Aptitude Test Battery*. Washington D.C.: National Academy Press, 1989.

Hoerr, John; with Hafner, Katherine M.; DeGeorge, Gail; Field, Anne R.; and Zinn, Laura. "Privacy." *Business Week*, March 28, 1988, pp. 61–65 & 68.

Howard, Robert. *Brave New Workplace*. New York: Elisabeth Sifton Books, Viking Penguin Inc., 1985.

Irving, R.H.; Higgins, C.A.; and Safayeni, F.R. "Computerized Performance Monitoring Systems: Use and Abuse." (typewritten) Revised February 21, 1986.

Labour Canada Task Force on Micro-Electronics and Employment. *In the Chips: Opportunities, People, Partnerships*. Ottawa: Minister of Supply and Services Canada, 1982.

Labour Arbitration Yearbook 1991. Vol. 1. Edited by William Kaplan, Jeffrey Sack, and Morley Gunderson. Toronto: Butterworths-Lancaster House, 1991.

Law Reform Commission of Canada. *Electronic Surveillance*. Working Paper 47. Ottawa: Law Reform Commission of Canada, 1986.

Law Reform Commission of Canada. *Human Dignity and Genetic Heritage*. Protection of Life Series Study Paper. Ottawa: Law Reform Commission of Canada, 1991.

Law Reform Commission of Australia. *Privacy*. Report No. 22, Vol. 1. Canberra: Australian Government Publishing Service, 1983.

Lehr, Richard I.; and Middlebrooks, David J. " Work-Place Privacy Issues and Employer Screening Policies." *Employee Relations Law Journal*, Vol. 11, No. 3, Winter 1985–1986, pp. 407–421.

Levitt, Howard A. "Employee Privacy: Part II, Practical Applications in the Workplace," *The Employment Law Report*, Vol. 2, No. 9, September 1981.

Linden, Alan. *Canadian Tort Law*. Toronto: Butterworths, 1987.

Linowes, David F. *Privacy in America: Is Your Private Life in the Public Eye?*. Chicago: University of Illinois Press, 1989.

Linowes, David F. "Employee Rights to Privacy and Access to Personnel: A New Look:," *Employee Relations Law Journal*, Vol. 4, No. 1, Summer 1978.

Louis Harris and Associates; and Westin, Alan F. *The Equifax Report on Consumers in the Information Age*. Atlanta: Equifax Inc., 1990.

Lyon, David. "Citizenship and Surveillance in the Information Age." Working Paper No. 23. Kingston: Queen's University, 1991.

Markoff, John. "Remember Big Brother? Now He's a Company Man." *The New York Times*, March 31, 1991, p. E7.

Marotte, Bertrand. "War Against Drug Testing Escalates." *The Montreal Gazette*, October 10, 1991, p. C2.

Marx, Gary T.; and Sherizen, Sanford. "Monitoring on the Job: How to Protect Privacy as Well as Property." *Technology Review*, Vol. 89, No. 8, Nov/Dec 1986, pp. 62–72.

Marx, Gary T. "Privacy and Technology." *The World and I*, Vol. 5, No. 9, September 1990, pp. 523–541.

McLaughlin, Mark. "An Attempt to Tether Electronic Workplace." *New England Business Journal*, October 1989, pp. 13–16.

Miller, Arthur, R. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: The University of Michigan Press, 1971.

Ministry of Labour. *Working in Ontario: An Employee's Guide to Workplace Law*. Toronto: Ontario Ministry of Labour, 1990.

Ministry of Labour Research Branch. *Electronic Surveillance: A Discussion Paper*. No. 21. Toronto: Ministry of Labour, 1979.

Newman, M., Marks de Chabris, G. "Employment and Privacy," *Journal of Business Ethics*, Vol. 6, 1987.

Ontario Human Rights Commission. *Policy on Employee-related Medical Information*. April 1990.

Oreskovich, Carlie. "Beneficial or Detrimental? Computer Monitoring Debate Rages." *Financial Post*, Vol. 79(36), September 7, 1985, p. C14.

Papp, Leslie. "Working Under the Electronic Eye." *Toronto Star*, July 27, 1991, pp. D1 and D5.

Piturro, Marlene C. "Employee Performance Monitoring ... Or Meddling?" *Management Review*, May 1989, pp. 31–33.

Pokorski, Dr. Robert. "New Technologies in Underwriting: Genetic Testing." *Canadian Insurance/ Agent and Broker*, January 1992, pp. 28–30.

Potter, Beverly; and Orfali, Sebastian. *Drug Testing at Work: A Guide for Employers and Employees*. Berkeley: Ronin Publishing, Inc., 1990.

Powell, Doug. "Who's Watching Over You?" *Computing Canada*, Vol. 15, No. 16, August 3, 1989, pp. 1 & 6.

Privacy Commissioner. *Annual Report Privacy Commissioner 1984–85*. Ottawa: Ministry of Supply and Services Canada, 1985.

Privacy Commissioner. *Annual Report Privacy Commissioner 1985–86*. Ottawa: Ministry of Supply and Services Canada, 1986.

Privacy Commissioner. *Annual Report Privacy Commissioner 1987–88*. Ottawa: Ministry of Supply and Services Canada, 1988.

Privacy Commissioner. *Privacy Commissioner Annual Report 1988–89*. Ottawa: Ministry of Supply and Services Canada, 1989.

Privacy Commissioner. *Privacy Commissioner Annual Report 1989–90*. Ottawa: Ministry of Supply and Services Canada, 1990.

Privacy Commissioner. *Privacy Commissioner Annual Report 1990–91*. Ottawa: Ministry of Supply and Services Canada, 1991.

Privacy Commissioner of Canada. *Drug Testing and Privacy*. Ottawa: Minister of Supplies and Services Canada, 1990.

Privacy Committee and Labour Council of New South Wales. "Guidelines for Telephone Usage Monitoring Systems/Telephone Information and Management Systems." *Information Bulletin*, Sydney, November 14, 1983.

Privacy Committee of New South Wales. *Electronic Vehicle Tracking*, Issues Paper No. 62, Sydney: Privacy Committee of New South Wales, August 1990.

Privacy Committee of New South Wales. *Employment Guidelines — The Privacy Aspects of Employment Practices in the Private Sector*. Sydney: Privacy Committee of New South Wales, 1979.

Privacy Committee of New South Wales. *Openness in the Employer-Employee Relationship to Ensure Fairness*. Sydney: Privacy Committee of New South Wales, 1979.

Privacy Committee of New South Wales. *The Privacy Bulletin*, Vol. 4, No. 1, June 1988.

Privacy Committee of New South Wales. *Screening for Drug Abuse — A Community Challenge*. Sydney: Privacy Committee of New South Wales, February 1988.

Reibstein, Larry; and Springen, Karen. "Spotting the Write Stuff." *Newsweek*. February 17, 1992, p. 44.

Report of the Standing Committee on Justice and the Solicitor General on the Review of the Access to Information Act and the Privacy Act, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, Ottawa, Queen's Printer, 1987.

Report on the National Symposium on Personal Privacy and Information Technology. Sponsored by the American Bar Association's Section of Individual Rights and Responsibilities Committee on Privacy and the American Federation of Information Processing Societies, Washington, D.C.: American Bar Association, 1982.

Robertson, David; and Wareham, Jeff. "Electronic Eavesdropping." *Union*, Vol. 4, No. 3, Winter 1990/1991, pp. 7–9.

Robertson, David; and Wareham, Jeff. *Technological Change: Air Canada Customer Sales and Service*. CAW Canada, March/April 1990.

Rothfeder, Jeffrey; Galen, Michele; and Driscoll, Lisa. "Is Your Boss Spying on You?" *Business Week*, Issue 3141, January 15, 1990, pp. 74–75.

Royal Canadian Mounted Police, *Drugs in the Workplace*. Ottawa: Minister of Supply and Services Canada, 1988.

Rush, Curt. "Thieves Are at Work — Stealing Time." *Toronto Star*, July 1, 1984, p. H1.

Sampson, Sandra T. "Privacy: The Invasion of the E-Mail Snatchers." *Datapro InfoSecurity*, Vol. 7, No. 4, April 1991, pp. 1–3.

Schiller, Zachary; Konrad, Walecia; with Forest, Stephanie Anderson. "If You Light Up on Sunday, Don't Come in on Monday." *Business Week*. August 26, 1991, pp. 68–70, 72.

Schreier, James W. "The Work Environment, Survey Supports Perceptions: Work-Site Drug Use is on the Rise." *Personnel Journal*, Vol. 66, No. 10, October 1987, pp. 114–118.

Science Council of Canada. *A Workshop on Information Technologies and Personal Privacy in Canada*. Ottawa: Minister of Supply and Services, 1985.

Shattuck, Cathie A. "The Tort of Negligent Hiring and the Use of Selection Devices: The Employee's Right of Privacy and the Employer's Need to Know," *Industrial Relations Law Journal*, Vol. 11 No. 1, Spring 1989.

Shattuck, John. "Computer Matching, a Serious Threat to Individual Rights." *Communication of the ACM*, June 1984, pp. 538–541.

Shepard, Ira Michael; Duston, Robert L.; and Russell, Karen S. *Workplace Privacy: Employee Testing, Surveillance, Wrongful Discharge, and Other Areas of Vulnerability*. Washington, D.C.: The Bureau of National Affairs, Inc., 1989.

Shepard, Ira Michael; and Duston, Robert. *Thieves at Work: An Employer's Guide to Combating Workplace Dishonesty*. Washington, D.C.: The Bureau of National Affairs, Inc., 1988.

Smith, Robert Ellis. *Privacy — How to Protect What's Left of It*. (Photocopy) n.p., 1979.

Smith, Robert Ellis. *Workrights*. New York: E.P. Dutton, Inc., 1983.

"Snoops Put a Strain on Employee Loyalty." Editorials, *Business Week*, Issue 3141, January 15, 1990, p. 94.

Southerst, John. "Managerial Vigilance Still Best Way to Put an End to Employee Crime." *Financial Post*, May 25, 1987, p. 23.

Standing Committee on Justice and Solicitor General. *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. Ottawa: Queen's Printer, March 1987.

Statistics Canada. *Canada's Unionized Workers: A Profile of Their 1987 Labour Market Experience*. Ottawa: Minister of Supply and Services Canada, 1991.

Stone, Dianna L.; and Kotch, Debra A. "Individuals' Attitudes Toward Organizational Drug Testing Policies and Practices." *Journal of Applied Psychology*, Vol. 74, No. 3, 1989, pp. 518–521.

Surtees, Lawrence. "Security Stifles Voice Mail Hack Attacks." *The Globe and Mail*, May 1, 1991, p. B4.

"Surveillance and Individual Privacy." *U.N. Chronicle*, April 1983, pp. 26–28.

Susser, Peter A. "Electronic Monitoring in the Private Sector: How Closely Should Employers Supervise Their Workers?" *Employee Relations Law Journal*, Vol. 13, Spring 1988, pp. 575–598.

Thacker, J.W. and Cattaneo, R.J. "The Canadian Personnel Function: Status and Practices." Paper presented at the administrative Sciences association of Canada Conference, Toronto, Ontario, June 1987.

The Information Web: Ethical and Social Implications of Computer Networking, Edited by Carol C. Gould. San Francisco: Westview Press, Inc., 1989.

Transport Canada. *Strategy on Substance Use in Safety-sensitive Positions in Canadian Transportation*. Ottawa, March 1990.

Transport Canada. *Information*. Ottawa, 1990.

United States Congress, Office of Technology Assessment. *Automation of America's Offices, 1985–2000*. Washington, D.C.: United States Government Printing Office, December 1985.

United States Congress, Office of Technology Assessment. *Genetic Monitoring and Screening in the Workplace*. Washington, DC: United States Government Printing Office, October 1990.

United States Congress, Office of Technology Assessment. *Mapping Our Genes — The Genome Projects; How Big, How Fast?*. Washington, DC: United States Government Printing Office, April 1988.

United States Congress, Office of Technology Assessment. *The Electronic Supervisor: New Technology, New Tensions*. Washington, D.C.: United States Government Printing Office, September 1987.

United States Congress, Office of Technology Assessment. *The Role of Genetic Testing in the Prevention of Occupational Disease*. Washington, D.C.: United States Government Printing Office, April 1983.

Venne, Rosemary Amelia. *Psychological Testing in Personnel Selection*. Kingston, Ontario: School of Industrial Relations Research Series, No. 8, Queen's University, 1987.

Ware, Willis H. *Emerging Privacy Issues*. Santa Monica: The Rand Corporation, October 1985.

Warren, Samuel D. and Brandeis, Louis D. "The Right to Privacy." *Harvard Law Review*, Vol. IV, No. 5, December 1890, pp. 193–220.

Watt, David. *Law of Electronic Surveillance in Canada*. Toronto: The Carswell Company Limited, 1979.

Watt, David. *The Law of Electronic Surveillance in Canada — First Supplement*. Toronto: The Carswell Company Limited, 1983.

Weitz, Mark S. "Biometric Systems: Better, But Still Pricey." *Datapro InfoSecurity*, Vol. 7, No. 5, May 1991, pp. 4–5.

Wells, Wayne, Walter, Robert and Calhoun, Robert J. "Potential Employer Liability for the Disclosure of Employee Information." *Akron Business & Economic Review*, Vol. 20, #3, Fall 1989.

Wertz, Dorothy. "Biomedical Research: Genetic Testing and Confidentiality." *The World and I*. September 1990, 523–541.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.

Wilson, David. "Trends in Information Society." *Computer Security Journal*, Vol. IV, No. 2, n.d., pp. 29–38.

9 to 5. *Stories of Mistrust and Manipulation: The Electronic Monitoring of the American Workforce*. Cleveland: Working Women Education Fund, February 1990.