THE EYES OF CAPITALISM: SURVEILLANCE IN THE WORKPLACE

A Study of the Issue of Employee Privacy

by

MARK DANIEL IHNAT

A thesis submitted to the Department of Sociology

in conformity with the requirements for

the degree of Master of Arts

Queen's University

Kingston, Ontario, Canada

March, 2000

Abstract

Employee privacy and surveillance in the workplace have generated a great deal of interest in the past, but the widespread proliferation of electronic communications and the increased intensity of employee surveillance have rejuvenated the issue of workplace privacy. This essay addresses the issues surrounding the definition of privacy, the social elements of surveillance in the workplace, current legal privacy legislation, and some union reactions regarding employee privacy. It is argued that the issue of employee privacy is an ambiguous one for it borders on the notions of freedom and resistance, and inclusion and exclusion. I contend that despite elements of intensified workplace surveillance, the issue of privacy becomes an issue of compromise and understanding.

The essay starts off with a brief introduction which outlines how employee privacy can become compromised in the workplace. In chapter two, various notions of privacy are discussed and privacy is located within a moral, economic, and social context. Privacy becomes defined as a concept based on control, separation, and data protection. I then argue that the complexities of privacy are related to economic, bureaucratic, and capitalist elements of the workplace, which include a discussion on the nation-state and discipline. Chapter three then focusses on three particular technologies and methods of surveillance, e-mail monitoring, video surveillance, and genetic screening, all of which are found within the workplace. In this chapter I argue that a discussion of privacy must incorporate the notions of trust, community, power, inclusion and exclusion, and the creation of the perfect worker. Finally, this essay investigates the ambiguous legal protection against privacy invasion and union reactions. I argue that the social concept of

privacy cannot be adequately protected within the legal domain. Also, the issues of privacy and the surveillance of employees are of significant concern amongst some unions, especially when the protection of employee data and the mental and psychological well-being of employees is at stake.

Acknowledgements

I would like to thank my supervisors, Professors Elia Zureik and David Lyon, for introducing me to the field of information technology, for their academic guidance, support, and patience. I would also like to thank Courtney, my sister Natasha, and my parents, for all their help, support, patience, and strength. Finally, I would like to thank Evert Hoogers, who provided me with a wealth of information and his time.

Table of Contents

Chapter 1 - Introduction

Cubicle Fortress Penetrated

Don't Even Bother Locking Your Door

The door to the office is closed and the curtains are drawn, in an attempt to assure oneself complete visual privacy and physical seclusion from coworkers and management. It is impossible for the curious prying eyes of others to see through these walls. How can anyone know what one is typing, whom one is e-mailing to, or what one is doing on company time? An anonymous staff member sits in his cubicle, typing love letters to his mistress. Unbeknownst to him, each letter is being printed out at the other end by management. Another employee surfs the World Wide Web on company time, exploring various web sites which are not work related.

Many employees assume that their surrounding walls and personal computers ensure privacy, isolation, and secrecy. But the walls are thin, the personal computers become impersonal, and their self-constructed cocoons of privacy ooze information that could, in the end, be evidence or leverage used for future job assessments and possible dismissals. E-mail messages have become binary bees, leaving their stingers after they have been sent, thereby providing electronic evidence for employers to investigate. Although e-mail messages are sent on the assumption of privacy, they lack adequate legal privacy protection and thus e-mail messages cannot be considered as private

correspondence and thus cannot stand up in court in either Canada or the United States (Lind, 1998:IT11). In Canada, the courts are "becoming more comfortable with electronic data," and it is almost routine to request the search and seizure of hard disk space (Lind, 1998:IT11). There is also limited escape from the beguiling eyes of video surveillance (Schuurman, 1995), infrared badge monitoring devices, and basic eye-to-eye observation. As well, surfing the Web can be problematic as every quick search and site visited adds crumbs to the "cookie" trail.[1] Even medical records which involve genetic testing become an employer's fortune telling cards, with the ability to predict one's medical future. Privacy has become an indescribable luxury in some workplaces, threatened by inquisitive and concerned management. However, in addition to violations of privacy within the workplace, employee privacy *poses* a possible threat for employers. If there is no knowledge of employee work habits and actions, too much privacy can become detrimental to employee and company productivity.

The workplace thus becomes a difficult area to regulate, because it is where one's private and public lives come together. But the regulation of the workplace has to do with the regulation of employees, and herein lies the major concern. The issue of privacy has become a complex point of debate as privacy as a concept cannot be merely relegated to the act of being left alone. Privacy becomes a concept that becomes intertwined with social, legal, and moral responsibilities and relations. Thus, one must understand the

---

[1] The term "cookie" refers to an Internet browser mechanism which allows various web sites to retrieve and record information regarding one's computer and one's Internet connection while online. The information found in a cookie can be retrieved without one's consent or knowledge.

issues surrounding workplace surveillance and the relationship of privacy. Only then, when privacy is revealed as a multi-disciplined, all-encompassing concept, can workplace surveillance be fully understood. What needs to be done is that privacy must be explored from several disciplines, and the history of surveillance in the workplace must be discovered. The impact of surveillance must also be investigated in terms of how the employee is situated within the work environment, and, finally, the legal and union responses must be explored in order to ground privacy as a common concern - to place the concept of privacy within the hands of the employee, albeit a difficult task.

Therefore, the goal of this essay is to research the workplace, and to determine the employee/employer relationship and the relationship between surveillance, the workplace and society - - a task which involves defining privacy and investigating the sociological circumstances of workplace surveillance. In the end, this essay is meant to be one of enhanced awareness. This essay outlines the dangers of workplace surveillance; it attempts to explore the legitimacy of workplace surveillance and its excesses; and it attempts to provide a building block towards privacy self-awareness. It expands and elaborates the often simplified privacy/workplace surveillance debate in order to point out the potential dangers of surveillance, but also to question total paranoia related to the workplace experience.

Who does the watching and why there is such a "need" for enhanced workplace surveillance are the major concerns for employees, their employers, and this thesis. The invasion of privacy becomes a crucial point of contention within the workplace, because it is a matter of deciding how far the limits of privacy should extend within the workplace.

It is a matter of deciding the focus of privacy that should and can be protected, how workplace privacy is being threatened, why privacy itself is such a threat to management, and how, if possible, we manage to balance the necessity for workplace surveillance, maximized employee output, and the protection of privacy. The limits of privacy depend on the definition of privacy and its application to the employment environment. As well, it is necessary to distinguish the right to privacy from the loss of privacy within the workplace. Legal protection depends on the various pieces of legislation found at the federal, and in Canada's case, provincial levels, that will protect the employee and the employer from counter claims. Such protection against the invasion of privacy can also be found in individual contracts and union/employer agreements. The methods of workplace surveillance involve e-mail monitoring, genetic testing, and other technological gadgets, such as video surveillance and infrared monitoring. Finally, the issue of workplace privacy and surveillance depend on finding a balance between employer and employee relations, and on challenging the distinct and not so-distinct overtones of social control.

Overview of Chapters

The essay is organized into four different chapters, tracing the development of surveillance in the workplace, the implementation of surveillance, the threat towards privacy, and legal and union reactions meant to deal with the invasion of privacy in the workplace.

The second chapter expands on the discussion of privacy and explores the theoretical aspects of surveillance, arguing that the birth and continuous growth of surveillance in the workplace are linked to a capitalist rationality. Chapter two expands on the definition of privacy to include not only philosophical and moral definitions, but also a social understanding. By constructing an understanding of privacy that includes various theoretical positions, while focussing on the issue of control, this chapter outlines the complexity of privacy. The chapter then shifts towards a theoretical exploration of surveillance by discussing modernity, the nation-state, the evolution of surveillance within and outside of the workplace, social control, discipline, and the economics of surveillance.

The third chapter examines the different methods of surveillance and their social and physical implications and the crucial relationship between privacy and the workplace. While the workplace and its employees are under the watchful eyes of the employer via surveillance, the methods and goals of surveillance have changed over time. This chapter examines the different modes of surveillance, outlining the unique characteristics of different methods of surveillance. Video surveillance, e-mail, and genetic screening are the three main methods of surveillance which are the focus of this study with each possessing a distinct feature. Genetic screening and video surveillance introduce an element of prediction in the workplace while the monitoring of e-mail allows for the interception of personal and non-personal messages, blurring the line between the public and private, and challenging the notion of proprietary rights. These three methods of surveillance represent an intensified form of surveillance as they are more controlling than

face-to-face surveillance. The chapter outlines the many aspects of privacy invasion in the workplace, addressing the issues of trust and private and public life. In addition, the chapter analyses the motivation behind surveillance, attempting to examine the various reasons behind the need for an employer to monitor an employee. The creation of a "perfect worker", the social relation of privacy, voyeuristic tendencies, and social control become the key components for instituting surveillance in the workplace. It is argued that although there might be a natural 'need' to implement a form of surveillance, there are other factors that must be considered. The collection of personal information through monitoring allows for an employer to mould an employee, to create an efficient workplace, and to control a workplace. Information becomes a commodity, an employee's leash, an element needed to distinguish deviance from normality, and ultimately can be manipulated as a form of control. The collection of personal information becomes an extension of the global community to which each of us continues to contribute to and feed from. We become victims of a self-perpetuated surveillance community.

Finally, chapter four is divided into three parts: the current public concerns regarding privacy, different Canadian legal avenues towards the protection of privacy and personal information, and the reaction of some unions towards the monitoring of employees. Using a 1993 Canadian survey on privacy, the degree of privacy concerns among Canadians is discussed, concluding that there is a general fear that privacy is being lost. As well, inadequate legal precedents are considered. The Canadian Charter, the Criminal Code and various other legislation fail to adequately protect Canada's citizens

and employees. Outdated laws fail to cope with an increase in surveillance and the improvement of existing technologies, especially in the private sector, which remains virtually unprotected. Finally, union responses towards employee privacy invasion have been somewhat effective, but limited. Various unions have attempted to incorporate protective measures in their collective bargaining agreements, but these provisions are limited and are slowly implemented. Equally important is the need to understand the goals of unions when it comes to protecting their employees. It is argued that unions have perhaps shifted their focus from the debate over employee efficiency towards protecting employee information. However, unions have yet to rank employee privacy as one of their main concerns, even though privacy complaints are common within the workplace.

Chapter 2 - Privacy: Defining the Boundaries

The Many Faces of Privacy - Part I: What it Is, What it is Not, and What it can Be

From Morality to a Commodity

From a social-psychological perspective, privacy has been associated with personal identity and the orientation of oneself to one's environment. Yehudi A. Cohen, as quoted in Derek McLean's book, suggests that "the need for privacy is one of the motive forces in the individual's orientation to the world around him...[one] of the functions of the ego is to control as needed the volume and intensity of stimulation from other people" (1995:10). Thus, privacy implies freedom and the ability to control one's surroundings and environment to some extent. Privacy also enables us to establish certain social distances depending on the nature of the social relationship. Based, to an extent, on Georg Simmel's and even Erving Goffman's work on social distance, Robert F. Murphy examined the Tuareg of the Mediterranean and their use of the veil. Focussing on the function of the veil to create social distance, Murphy made a general conclusion that "social distance pervades all social relationships," and that people in general insulate themselves. They do so by protecting themselves from others in terms of withholding information and maintaining a degree of privacy which is "concretely accomplished through distance setting mechanisms" (Murphy, 1984:51). It is a matter of distancing one's self from certain individuals, and when the time is right, allowing others into one's

personal space.

Privacy becomes an individual social action where there is a need for one to establish privacy oriented relations with others and one's environment. But such privacy then becomes relative, and perhaps misguided, since relationships with others govern us, and we are further bound by larger organizations with their inherent methods of social control. One's ability to completely regulate privacy can only exist if all parties and all social relationships are built on some sort of mutual understanding. This has become increasingly difficult, however, as Edward Shils claims, because our relationships with others and especially with organizations have drastically changed. The expansion of organizations has created difficulties, in terms of being able to govern and protect vast collectivities (in McLean, 1995:23).

With the expansion of organizations comes the expansion of surveillance and thus, an increase in social control. Due to the changing structures of modern society and the birth of the nation-state, large-scale organizations developed the ability for intensive systems of mass surveillance, with the result that the management of personnel and private information becomes a crucial aspect of social control (Rule, 1973). What we are left with is a paradox, where one must relinquish information and privacy for the good of the organization. But such compromises in privacy are also done for the good of the individual. The relinquishing of information has to do with the concept of a privacy relation, one that involves exclusion and inclusion (Lyon, 1994). Nonetheless, the paradox traps those who wish to have the best of both worlds - that of privacy and that of safety and security. The information collected from individuals can be used to "protect

the interests they represent...(as) information is never a neutral commodity, but entails advantages or disadvantages to one side or the other" (Rule, 1973:311). Privacy can thus be a double edged sword: it enables and disables the individual.

Privacy is relinquished, protected, desired, needed and sacrificed, but this hardly explains what privacy *is* and what it is *not*. Privacy can be considered a moral right, a protection of one's interests, and a control over access to personal information and limited access to an individual. The constant desire for privacy demonstrates the need to exercise a moral right. In terms of the workplace, "men's craving for privacy is easy to understand, for the ability to withhold information may mean the ability to escape the reach of corporate control," but as Rule further points out, individuals desire privacy for its own sake, "simply for the inherent satisfaction of protection from the idle curiosity of others" (Rule, 1973:331). However, is the mere avoidance of curious eyes and the satisfaction of retaining privacy, enough to establish the moral right of privacy?

Privacy must be given a higher value, a higher status. According to Charles Fried (1984), privacy is a good technique for furthering fundamental relations such as trust, friendship, and love. Without privacy, Fried argues, these relations would not exist for they require a "context of privacy or the possibility of privacy" (Fried, 205). All three mentioned relations are common, in the sense that they are built on a moral conception "of the basic entitlements and duties of persons in regard to each other". This idea of common relation means that there must be a recognition of an individual's basic rights of maximum liberty with respect for the liberty of all (Fried, 1984:206). Thus, the principle of morality establishes equal liberty for each person to define and pursue one's values free

from undesired impingements by others (Fried, 1984:207).

Morality becomes a universal liberty that allows one to do whatever one wishes as long as another person does not have any "good" reason to prevent such an act (Benn, 1984). This concept becomes problematic for it is based on the notion that there is universal good and evil. However, the principle of morality is not an absolute value system, but rather a spectrum of values based on ethics. Values pursued are consistent with "an equal right of all persons to a similar liberty to pursue their interests" (Fried, 1984:206). Also crucial is the concept of respect, which is what one must possess in terms of observing another person's basic rights and observing the principle of morality. Thus, the morality that underlies these particular relations of trust, friendship and love, is the "constraint of respect for the privacy of all" (Fried, 1984:207).

Privacy, according to Fried, is therefore established through a relationship with others based on respect, moral considerations, and a mutual relationship of understanding between individuals. The existence of love, trust, and friendship depend on such a notion of privacy; however, should privacy exist without these relations it would be open to massive scrutiny. Privacy is the personal control of information which allows the individual to monitor the quality and quantity of information surrendered. Privacy also allows an individual a degree of personal liberty. With a guarantee of privacy, one can indulge in personal freedom, saying what one wants without worrying about third parties listening in. Privacy gives one the freedom of surrendering information with the hope that information is not intercepted. Thus, individuals would value privacy even if there was no love, friendship or trust, "yet they leave privacy with less security than we feel it

deserves; they leave it vulnerable to arguments that a particular invasion of privacy will secure to us other kinds of liberty which more than compensates for what is lost" (Fried, 1984:211). Beyond personal liberty, privacy allows for the control of information and establishes a certain context for social relations based on mutual respect. However, respect for others also assumes that one can override curiosity which some, such as Alan Westin, argue is a universal human trait that provides an important function. Curiosity circulates information as people are on a 'need to know' basis which is necessary for the establishment of relations with others. This notion of curiosity and respect promotes group norms and expresses hidden desires through vicarious experiences (Westin, 1967). It is a matter of containing curiosity without killing it, and simultaneously maintaining respect.

The control of information however, does not fully explain privacy nor its implications. To protect personal information from others is not the same as keeping a secret, while claiming that privacy is always desired does little for the individual stranded on a deserted island. There are rules, exceptions, and limits for privacy and the key is to decide when and where these rules apply.

However, privacy goes beyond the philosophical inklings of morality, for privacy is also grounded in the more practical notion of economics. Privacy has become a commodity, part of the trade-off equation, where privacy is traded in return for better levels of service or products. And thus privacy ventures onto a slippery slope, where as Paul-Andre Comeau suggests, "we are lured...by the new technologies in their attempt at putting a dollar figure to each piece of information." (Comeau in House of Commons

Standing Committee,1997:10).[2] Caught within this trade off equation, it is argued that privacy does not even exist any more as we know it. C. C. Gotlieb argues that most people do not even care about privacy any more because the sacrifice of privacy for practical purposes is seen as beneficial (Gotlieb, 1996:156). Gotlieb argues that we have given up our privacy, sometimes willingly and sometimes reluctantly, but nonetheless we have given it up and in exchange we reap the financial (credit limits, licenses) and the social benefits (citizenship) (Gotlieb, 1996). The relationship that has thus been established between individuals and privacy has rendered the definition of privacy, as we know it, virtually obsolete. Privacy and privacy laws are now obsolete because it is confidentiality which is of prime importance and confidentiality has become a commodity. It is not the act of the invasion of privacy or the act of relinquishing information that matters, the majority of people are more than willing to look past such annoyances, but now the concern is how is that information is used and distributed. The management of information has made confidentiality a commodity rather than privacy. Gotlieb also argues that we have it all wrong when we talk about privacy and the increase of social control. He argues that the techniques of surveillance in the workplace and elsewhere "are being implemented because people want the benefits that flow from the techniques, and that their adoption should be viewed, not as social control, but as responses to expressed needs and market forces" (Gotlieb, 1996:164). The need for social control or surveillance is expressed by the 'needs' for certain benefits which result from the sacrifice of privacy. Essentially, you get out of the system what you put in it. But are

---

[2] Paul-Andre Comeau is the Privacy Commissioner of Quebec.

the benefits of privacy so great as to overlook other issues? An employee who has lost his job because of workplace monitoring or an individual who cannot obtain a loan because of a faulty bad line of credit might disagree.

The moral, philosophic, and economic arguments stated above regarding privacy merely scratch the surface, but they pose several interesting questions and open up the privacy debate. Is privacy an individual classification, is it an aspect of trust, or is it simply a commodity? These complexities of privacy and their relation to the workplace must be further explored, especially in terms of the relationship between privacy and information. Thus, we must explore the sociological aspects of privacy, information, and data protection.

The Many Faces of Privacy - Part II: The Puppet or the Puppeteer

Controlling Information and Privacy

Found in many forms, informational privacy generally means that there is a controllable boundary between individuals involving the control of information, and the control of physical privacy. Privacy and its boundaries are found in many different "states" such as individual solitude, intimacy, anonymity and reserve (Westin, 1967:31). Solitude is found when an individual can physically remain outside of, or separated from, a group or from the observation of others. In contrast, with intimacy, the individual "claims and is allowed to exercise corporate seclusion"(Westin, 1967:31). In an intimate

relationship, all those involved can be upfront and frank with each other based on the closeness of the relationship. Anonymity occurs when one can act in public places, but is still allowed to seek refuge from identification and surveillance because the individual is a "stranger" in the public domain. Reserve, on the other hand, refers to the ability to set up a form of psychological barrier where one is able to hold back information, thus creating a "mental distance" (Westin, 1967:32). Based on these four states, privacy functions to create personal autonomy, emotional release, self-evaluation, and protected communication, all of which provide the individual with an arena for private reflection (Westin, 1967).

Privacy provides a personal safe-haven for individuals where secrets can be withheld, opinions can be expressed, and confidentiality is of utmost importance. However, this does not necessarily imply that secrecy and confidentiality alone mean privacy. One can be secretive and maintain confidentiality, without maintaining privacy. Confidentiality provides only the means of protecting information by keeping it secure from prying eyes, while secrecy is a less intimate form of privacy. Julie Inness argues that we lack privacy as a fundamental right or claim because we cannot morally control non-intimate information (Cavoukian, 1995:30; Inness, 1992:60-61). The protection of information, mainly legal protection, allows information to remain confidential, but secrecy has no such protection. Inness associates privacy with the basic notion of intimacy, claiming that intimacy is the core to privacy. Similar to Fried's argument on privacy where respect and to some degree intimacy are crucial for privacy and specific social relations, Inness contends that intimacy is important regarding access to

information, physical access to individuals, and certain activities a person may undertake such as marriage (Inness, 1992:74). Fried argued for a "commodity theory" of intimacy "where information is intimate when it functions as a commodity from which relationships can be constructed" (Inness, 1992:81). In a relationship based on respect, individuals relinquish certain information to another person or their partner. Inness however, argues that the sharing of information alone does not constitute intimacy, nor does it constitute a close relationship. For instance, one can share information with one's mechanic, information that is most likely only known by that individual, yet this does not signify an intimate relationship with one's mechanic (Inness, 1992:82). Inness concludes that intimacy is not merely the sharing of information, but rather information "is intimate if and only if it is understood to take its meaning and value from our love, liking or care" (Inness, 1992:83). Therefore, the sharing of information in a relationship is only intimate if one *values* the access of intimate information. The value of intimacy is drawn from a personal view, from those involved in the relationship. Therefore, privacy "amounts to the state of the agent having control over decisions concerning matters that draw their meaning and value from an agent's love, caring or liking" (Inness, 1992:91). Privacy claims allow for control over intimate decisions. This leads us to the argument regarding privacy as the ability to control information, or the ability to deny access to an individual through physical or psychological separation or isolation.

Inness states that privacy must be looked at from two different perspectives. On the one hand, privacy can be antithetical to publicity; its function is to separate individuals from others, "restricting the access others have to particular areas of her life [and]

accordingly [it is] a claim to privacy [which] becomes a claim to have these areas of life separated from the world" (Inness, 1992:5-6). On the other hand, Inness points out that privacy, referring to privacy and access-control, might not be necessarily in opposition to publicity, but rather it provides an individual with control over certain aspects of one's life. Separation-based theories of privacy describe privacy as an attempt to separate oneself from the community. However, such solitude is the result of the detrimental side of privacy, according to Deckle McLean. Access-control privacy, the ability to limit the physical access and to avoid outside observation, can be dangerous because to be shrouded in mystery results in community fear (McLean, 1995:62)[3]. In consequence, there must be a balance of access-control privacy, where control is limited yet effective. An excess of access-control can create "tension that comes from having unknowns in a community, or the instability that results when all community units are private" (McLean, 1995:63).

Inness argues however that the separation-based definition of privacy is inadequate. Even though limited access might result in privacy, such separation does not mean that privacy is solely based on limited access. Separation from others does not necessarily achieve a form of privacy (Inness, 1992:43). To be accidentally locked in a room where one can neither be looked at nor listened to does constitute privacy in terms of being separated from others. However, the value of that person's privacy is a negative one, for that individual would not want to be necessarily locked up. Thus, their desire

---

[3] McLean's point touches on a point that Stephen Nock (1993) argues, that of community. However, Nock, as we shall find out later in the essay, associates the mysteries of individuals to an increase of privacy which is why we need surveillance.

would be for a loss of privacy, for their space to be invaded, for the door to be unlocked (Inness, 1992:42). The person imprisoned in the room "no longer experiences privacy because [they lack] control over who looks at [them]" (Inness, 1992:43). In this situation, there is an undesirable lack of privacy even though one is separated from others. Separation is a neutral concept until it is put into a certain context. Thus, privacy becomes neither desirable nor undesirable. Also, if privacy is based solely on separation, no matter whom one encounters, privacy would be lost (Inness, 1992:43-44).

As for control-based explanations of privacy, it is not only a matter of hiding in a room with the door shut or denying physical access to others, but dealing with the fact that an individual has information that can be surrendered when he or she wishes. Therefore, one can be part of the community and yet remain private by not sharing certain information. Inness points out that control-based explanations of privacy succeed where separation-based theories failed. Controlling one's personal information is a positively valued condition and a form of autonomy. Control-based privacy allows one to be in the presence of others without losing privacy, as one can allow others into an intimate relationship where privacy and control of information are compromised. Control-based privacy can deal with privacy violations and threats that do not necessarily have to do with access (Inness, 1992:47-51). Thus, in order to define privacy, it is a matter of deciding if privacy is an act of separation or an act of control. Inness argues that privacy is a value based on both separation and control. Therefore, the value of the experience is important in determining if privacy is being achieved.

Inness' arguments regarding separation-based and control-based forms of privacy,

and Fried's notion of trust provide some of the groundwork for privacy in the workplace, even though these definitions of privacy do not deal specifically with informational privacy. In terms of the workplace, the monitoring of an employee does not enable her to ultimately control what information is being collected. Granted an employee can modify behaviour so as to appease those who are doing the monitoring, but this does not necessarily allow the employee to control information, either work or non-work related. Also, it is not a viable option for an employee to separate himself and his information from co-workers and management, as management needs a certain degree of employee information in order for the company to operate efficiently. The sharing of information within the workplace creates a knowledge-based community. The exchange of information and the knowledge of employee work habits becomes an important aspect of running a business. However, whether the sharing of information creates an equal knowledge-based "partnership" between employee and employer is questionable. The type, amount, and value of information that flows between both parties becomes a crucial point of contention. The sharing of information does not automatically supersede employee privacy or the control of private information, but rather adds a contentious element to the employee/employer relationship.

There is also a relationship between trust and privacy that must be accounted for. The issue of privacy and the world of strangers we live in has been appreciated ever since the work of Georg Simmel (Webster, 1995:56). Simmel pointed out how "disorienting and also often liberating the transfer from closed community to a world of strangers can be" (Webster, 1995:56). The fragmentation of society might depersonalize individuals,

but it might also empower them, freeing them from social structures and institutions. Frank Webster claims that "we have emerged from a world of neighbours and entered what has increasingly become one of strangers...here we have the old theme in social science of a shift from community...to associations which involve the mixing of people unknown to each other" (Webster, 1995:56). Trust is not necessarily a premise for privacy, but as Nock (1993) would suggest, a lack of privacy has increased trust through surveillance.

Nock claims that we have more privacy now than ever before, and thus we live in a world of strangers. Thus, Nock suggests that through the use of surveillance and the maintenance and verification of reputations that an element of trust can be established and strangeness eliminated. Therefore, surveillance is the cost of privacy (Nock, 1993:1). Privacy grows as long as the population grows, and thus there is a need for surveillance. His claim of too much privacy is an interesting departure from the more common arguments of a loss of privacy. As William Bogard argues, Nock's claim of too much privacy is a good one and saying that "information compensates us with a disenchanted form of trust in societies where privacy has become the predominant experience," is not wrong, but he fails to say that privacy or strangeness "itself comes in informated forms today" (Bogard, 1996:149). Bogard argues that information "simulates the social in its entirety," and that privacy still exists, but is now cleaned up, constructed, and is part of a hyper-controlled experience (Bogard, 1996:149). It is not that we have necessarily lost trust and privacy, but that privacy has changed; it is a different form of privacy from the one we used to know. Trust and privacy now become part of a simulation model where

"information networks substitute what 'passes' for a society based on reciprocity...and a digital simulacrum of the social order" (Bogard, 1996:149). Privacy now becomes a construct, an informated privacy ,"a cold simulacrum of privacy," which finds itself in a virtual world, not a world hidden from surveillance, but an "already staged, programmed isolation and strangeness"(Bogard, 1996:149).

Another aspect of privacy that must be noted is the relationship between privacy and protection. By this I mean the protection of information and protection against "unwarranted access or disclosure," as opposed to privacy being seen as a "state that one might seek to attain" (Gandy, 1993:194). In this case, privacy becomes a protection against threats and becomes a dimension of power where, as Kenneth Laudon suggests "privacy is a value which describes a power differential between the actor who seeks access and the individual who seeks to limit it" (Gandy, 1993:194). The relationship of power demonstrates a continuum with individual informational moral supremacy at one end and "complete supremacy of the organization and its needs for efficiency," on the other (Laudon in Gandy, 1993:194). The notion of informational control becomes challenged by efficiency. Within the workplace, the employee constantly and implicitly provides work performance information as well as non-work related information during any given day. The control of that information is what becomes a major concern for the employee in addition to the explicit and implicit measures of monitoring and surveillance.

Privacy and its Relationship to Surveillance and the Workplace

Modernity, Modern Society, and Surveillance

The enhancement of surveillance is closely related to the development of the nation-state, the nature of capitalism, and industrialism. The formation of the nation-state and its encompassing relations, gives a brief glimpse into modernity and the complexities of modern history (Giddens, 1985:34). An appropriate explanation of modern society and modern institutions, according to Anthony Giddens, requires a diagnosis of modernity, an analysis of "society", an explanation of disembedding mechanisms, and the reflexive appropriation of knowledge (Giddens, 1990:10-53). First of all, Giddens argues that modernity is "multidimensional on the level of institutions," in that both industrialism and capitalism are components of modern capitalist society and of the nation-state (Giddens, 1990:12). Modernity is irreducible to either capitalism or industrialism, but embodies a combination of both. Secondly, "societies" as we know them, should be referred to as nation-states, incorporating the intricacies of the nation-state and its relations with political power, surveillance, and citizenship. Nation-states should be characterized as social communities which radically contrast with pre-modern states (Giddens, 1990:13). However, both society and nation-state are not synonymous terms, but rather the "nation state is a particular kind of society, one created very recently in world history" (Webster, 1995:58). As Webster explains, Giddens' concept of the nation-state "must be examined as an artifice...the nation state is *not* a 'society', but a particular type of society that has

distinctive characteristics" (Webster, 1995:58). With this notion of society, it must also be understood that social systems deal with the problem of order through time-space distantciation - "the condition under which time and space are organised so as to connect presence and absence" (Giddens, 1990:14). The problem of order has to do with the integration of time and space. There is an intimate connection between modernity and the transformation of time and space because the coordination of time allows for the control of space (Giddens, 1990:18). With the organization of time and the control of space, organizations and modern states are able to connect the local and the global, expanding their reach. The result is globalization and the expansion of capitalist society (Giddens, 1990:18).

Thirdly, the disembedding of mechanisms is the "reorganization of social relations across large time-space distances" based on symbolic tokens, expert systems, and trust. As individuals, we put trust into certain symbolic items, such as money, which essentially functions as a bracket for time and space. Money acts as a bracket for time and space because the presence of individuals is not necessary during transactions, and money itself is trusted because it has an inherent known value. Similar to money, forms of identification, or using Nock's terms, ordeals and credentials, become mediators and signifiers of trust. Time and space are no longer problematic as these symbolic items replace an element of interaction between individuals. Expert systems are organized environments where external, most likely unknown individuals, have put their knowledge into creating one's environment. Thus, expert systems are disembedding mechanisms because "they remove social relations from the immediacies of context" (Giddens,

1990:28). Surveillance helps this reorganization of relations through the collection of information. The information gathered grounds these symbolic items, giving them credibility. Finally, modern societies and modernity are involved in the reflexive appropriation of knowledge which involves the monitoring of one's self. Giddens argues that the "reflexivity of modern social life consists in the fact that social practices are constantly examined and reformed in the light of incoming information about those very practices, thus constitutively altering their characters" (Giddens, 1990:38). It is the continual generation of knowledge and the circulation of said knowledge, that provides constant change. It is not a matter of dealing with what is new, but rather a matter of reflecting on what is known and thus, never being certain if knowledge will be revised.

It has been commonly assumed that the late twentieth century marks the era of information. However, Giddens argues that modern societies have always been predominantly information societies, with the basic recording of information already being performed. Giddens' "theorisation leads one to argue that the heightened importance of information has deep historical roots," and does not signify a necessary break in history or break from other systems (Webster, 1995:52)[4]. The nation-state represents a society concerned with the constant surveillance of its citizens through the gathering and recording of information. The key difference in modern societies compared to pre-modern societies, is the increased intensity and the intrusiveness of modern day surveillance and data collection. In order to understand the reason behind the

---

[4] Mark Poster's (1990) argument of a break in history with the mode of information is an important point and one that will be discussed later in the essay.

enhancement of surveillance in the nation-state, it is important to clarify the development of the nation-state and its relations to capitalism and industrialism.

Modern capitalist society must be understood as a relationship between capitalism and industrialism. Modern society is no longer reducible to either capitalism or industrialism, for the nation-state, according to Giddens, involves both industrialism and capitalism and the forming of a 'capitalist society'. The nation-state is a relatively new type of society emerging over the last four centuries with the expansion of industrial capitalism and globalization. The connection between capitalism and the nation-state is based on the European state system being able to finally accommodate capitalist accumulation. Although capitalist accumulation was predominant from the sixteenth to the early nineteenth centuries, it was the changes in class-divided societies in terms of time-space organisation, not necessarily the centralisation of state power, which furthered the connection between capitalism and the nation-state (Giddens, 1995:188). The late eighteenth and early nineteenth centuries marked the beginning of the capitalist and nation-state phenomena with the commodification of time, the "wholesale transformation of labour into wage-labour," and the transformation of the city-countryside relation allowing for the creation of one urban space.

The relation between the nation-state, capitalism and globalization is based on the concept of 'world time'. World time, a concept introduced by Eberhand, refers to a sequence of events that can have potentially different consequences in different phases of world development (Giddens, 1995:167). Hence, there are connections between societies of differing structural types - referred to as time space-edges (Giddens, 1993:191). These

connections are similar social events which might have "quite dissimilar implications or consequences in different phases of world development"(Giddens, 1995:167). Giddens argues that the similarities between societies result in different consequences. These consequences depend on how societies became shaped by 'outside' influences and how different societies were able to deal with the bracketing of time-space (Giddens, 1987:153). Thus, different societies have spanned different lengths of historical time, but as societies overlap in existence, they exist along time-space edges. Capitalism, for example, has injected a further set of such time-space edges, existing along the time-space edges with class-divided and tribal societies (Giddens, 1995:168). Thus, with these connections, capitalism has initiated "the creation of an intersocietal system that is truly global in scope" (Giddens, 1995:168). Differing from traditional societies and absolutist states, the nation-state involves the delimitation of territorial boundaries and the dissolution of the city/countryside relations. Fluid boundaries now become defined along with the creation of an urban space. Polyarchic nation-states rely on high administrative concentrations, achieved via surveillance and "the altered nature of the dialectic of control" which such intensified surveillance produces (Giddens, 1985:4). Based on the combination of industrialism, which includes the use of inanimate sources of material power, the mechanization of production, the manufacturing of production and the centralized workplace, and capitalism, which involves the commodification of labour and production, the nation-state and its administrative power are formed. Essentially, the "commodification of labour-power...is a phenomenon that directly connects the class system of capitalist society with industrialism as a form of production" (Giddens,

1985:142).

The expansion of administrative power is another basic point of connection between industrialism and capitalism. Writing and the keeping of records have always been modes of administrative tabulation, and not necessarily a representation of speech (Giddens, 1985:41). Writing has its own distinctive characteristics; it is an independent mode of language-use. Giddens argues that sentences "have a predicative character... [which] furnishes them with the capacity of reference" (Giddens, 1985:42). The gathering, storing, and use of information "about social activities and about events in nature...is fundamental to the existence of organizations" (Giddens, 1985:46). Such extensive administrative power, based on the expansion of surveillance, allows for the organization and coordination of human conduct in the workplace, as well as outside of the workplace. Surveillance becomes crucial in the coding of information as well as an essential element of power. According to Giddens, "administrative power can only become established if the coding of information is actually applied in a direct way to the supervision of human activities, so as to detach them in some part from their involvement with tradition and with local community life" (Giddens, 1985:47).

However, it is the impact of electronic communications on the time/space relationship which has facilitated administrative power in a capitalist society. The distance between point A and B, and even the distance between time interval A and B have become compressed. By controlling space, modernity tears space away from place, as space can be represented without referring to a certain locale (Giddens, 1990:19). Traditional time and space relations took place in particular locales, but capitalism alters

these relations, turning time and space into commodities (Tucker, 1998:113). Place, the physical and symbolic locale, "loses its particularity and becomes a form of "fictitious capital," as space becomes commodified - sold and bought like any other commodity" (Tucker, 1998:113; see also Giddens, 1987:150). The tearing of space from place also involves the separation of the home and the workplace, which is "only one aspect of broader processes of time-space regionalization involved in modernity" (Giddens, 1987:151). New categories of home and work are created through the transformation of space into a commodity and new relationships between the public and the private emerge. The needs of capital become the dominant force as new spaces, such as modern urbanism, are created to adapt to these very same needs. As Kenneth Tucker summarizes, "temporal and spatial processes wrought by capitalism shape how everyday life is experienced, while creating new categories of home and work" (Tucker, 1998:113).

The importance of separating time and space, the ability to separate "immediate communication from presence," allows for institutions to organize across time and space and thereby "initiate developments in modern culture that...are basic to the emergence and consolidation of the nation-state" (Giddens, 1985:14). It is the formation of the nation-state that, in the end, has reconstructed forms of power, discipline, and administrative order based on intense surveillance. Older bases of power, such as absolutism and despotism, can be considered obsolete with the emergence of the nation-state and improved communications. As Giddens points out, "the accumulation of relevant information on disparate and geographically dispersed people becomes an imperative aspect of any government's aim of holding such people together within one bounded

territory, the nation state" (in Lyon, 1988:97-98).

The nation state has intensified surveillance, expanding on the printed material that recorded events to present-day electronic communications. Printing enlarged the administrative power of the state, as data collection became "part of the day-to-day operation of the state, although of course not limited to it" (Giddens, 1985:179). What is of key importance is the increase of stored records, records which were no longer merely tax records and population statistics, but also included "moral statistics" which referred to suicides and divorces. These statistics became "complete", excluding no one and incorporating all aspects of day-to-day life and these characteristics of surveillance could now be implemented with greater intensity in the workplace. Thus, with the storage and control of information, surveillance is considered "the mobilizing force behind administrative power...[and] the primary means of the concentration of authoritative resources involved in the formation of the nation-state" (Giddens, 1985:181).

This intense surveillance can be found in the workplace, which, with the given "dynamism which the insulated economic sphere injects into other institutional arenas," will have a great impact on other areas of life (Giddens, 1985:145). The focus on the workplace is linked to the centralization of the workplace caused by industrialization, where "manufacturing operations can be concentrated and co-ordinated" (Giddens, 1985:144). Giddens' work becomes quite useful when looking at the workplace, as he himself, according to Webster, "does not ignore the part played by capitalist endeavours, stating tartly that 'surveillance in the capitalist enterprise is the key to management'" (in Webster, 1995:71). Expanding on Giddens' work, Webster argues that surveillance has

gone beyond the shopfloor, including everyone in the corporation, which is a requirement for effective corporate activity (Webster, 1995:72). Such a discussion of Giddens by Webster on surveillance leads him into the common, and soon to be discussed, topics of Taylorism and self-discipline.

Finally, the nation-state has become a crucial point in the development and organization of people's identities. The nation-state embodies modernity, fragmentation, individuality, and identity. In this deeply historically rooted information society, in what Giddens refers to as "high modernity," the contemporary world is built around heightened surveillance and the nation state (Webster, 1995:52). All states have been information societies but with its "high degree of administrative unity," the nation-state brings the gathering and storage of information to a higher pitch (Webster, 1995; Giddens, 1985:178). Also, in addition to the convergence of time, space and administration, the relationship between warfare, internal pacification, and identity is a crucial one in the explanation of surveillance in the nation-state. With the waging of war, there has been a need for the nation-state to monitor its citizens, to secure and safeguard its population, and to become informed of the identities of the populace. Thus, citizenship rights are achieved where a contractual agreement with the citizens of the nation-state is created. Surveillance has been propelled by this need for internal pacification (Webster, 1995:68). As Webster nicely summarizes, "it is the extension of the nation-state and its intimate concerns with war and defence, in the growth of citizenship rights and duties, and in the extension of corporate capitalism...that we can see what may be better termed, not the 'information', but the surveillance society'"(Webster, 1995:73).

Beyond the Prison Walls

With the expansion of surveillance and administrative power, the issue of privacy becomes an increasingly crucial concern. Discipline and power become intertwined with surveillance, while the gathering and storage of information via increased surveillance, allows for the categorization and classification of individuals. For Michel Foucault, the historical process leading toward an increase in surveillance and the classification and categorization of individuals can be linked to methods of punishment. These methods have evolved from the "crude" spectacle of punishment towards the adoption of disciplinary practices. With this change in punishment, the criminal body finds itself involved in a new relationship, where the body is no longer property which is "owned", but rather part of the machinery of the discipline of power. The abandonment of public executions "marks a slackening of the hold on the body," and the body now becomes "caught up in a system of constraints and privations, obligations and prohibitions" (Foucault, 1979:11). Now the punishment of criminals results in confining prisoners to cells, as the body of the condemned person becomes "the property of society, the object of a collective and useful appropriation" (Foucault, 1979:109).

With this method of penal punishment, the prisons themselves exemplify disciplines of power, as the body becomes part of a larger organized structure, part of a new order. The prison becomes a technology of power, where power is not the prerogative of the dominant class and cannot be held, but rather is ubiquitous and all encompassing, independent of those who exercise it. The prison, and in Foucault's case

the Panopticon, is an all-seeing, self-regulating prison, providing a prime example of the technology of power "realized through the practice of disciplinary classification and surveillance" (Gandy, 1993:9). With the Panopticon, the discipline of power allows for the arrangement of bodies and time within a physical environment. It is not merely assigning bodies to a specific timetable, but rather, the use of time is exhausted, as it becomes a "question of extracting, from time, ever more available moments and, from each moment, ever more useful forces" (Foucault, 1979:154). Within the prison, the prisoners can be constantly monitored. It is this surveillance that brings power, as discipline becomes an integrated system "linked from the inside to the economy" (Foucault, 1979:176). Discipline creates an effective machine, within prison, as the body can be placed, moved, and monitored. Individuals are "created" in terms of being objectified and subjected to disciplinary power which regards them as "instruments of its exercise" (Foucault, 1979:170). Thus, discipline and power are crucial elements in the expansion of surveillance.

Discipline, although not situated or identified by one institution alone, brings the effects of power to the most minute elements of everyday life, expanding the distribution of power relations throughout society (Foucault, 1979:216-217). Bodies are surveilled not only in prison, but also outside the walls of the prison, for the Panopticon applies in other institutions such as hospitals, clinics, and factories. Oscar Gandy expands the concept of the Panopticon, arguing that the panoptic sort applies even beyond the walls of any institution as individuals become objectified through surveillance and the discipline of power. Thus, a body of knowledge is accumulated regarding these bodies/criminals/

patients, which allows for the classification and categorization of individuals, as well as the comparison of these individuals to each other and the norms of society, consequently validating or disqualifying individuals. Time and space have been ordered via the Panopticon and discipline as power. The control of the body, the control of groups and the control of knowledge have been brought together. The Panopticon "locates individuals in space, in a hierarchical and efficiently visible organization" (Foucault, 1984:19). The prison has become a technology of power where "the power to punish, which no longer dares to manifest itself openly, silently organizes a field of objectivity in which punishment will be able to function openly as treatment and the sentence be inscribed among the discourse of knowledge" (Foucault, 1979:256). This discipline of power and power relations, does not solely stay within the prison, but rather flows throughout society, penetrating our everyday lives.

Information Capitalism

Similar to Giddens' argument regarding capitalist society, Rob Kling and Jonathan P. Allen link the new computer technologies and large scale record keeping to *information capitalism* (Kling and Allen, 1996). Dealing with the internal aspects of organizations, information capitalism links both the information and traditional dynamism of capitalist enterprise (Kling and Allen, 1996:107). Information capitalism is a "set of management practices that encourage the use of data-intensive techniques and computerization as key strategic resources of corporate production" (Kling and Allen,

1996:127). The constant pursuit of information explains modern society's growing interest in extensive surveillance and the establishment of indirect relationships between individuals, where everyday activities are carried out with people who are not seen or even known to exist (Kling and Allen, 1996:114). It is not enough to explain the drive behind surveillance and the accumulation of information as a mere need, or improvement, or as an expansion of bureaucracy. Instead, surveillance is a strategy used to maximize the use of technology in society by placing more weight on the "internal configuration of organizations and the strategies and interests pursued" (Kling and Allen, 1996:112). Surveillance is not simply needed to "enforce the norms of client behaviour or to improve bureaucratic efficiency" (Kling and Allen, 1996:107). The development of new surveillance systems and information capitalism is done through an internal restructuring of corporations, and the creation of data-intensive management techniques important for information capitalism.

The formation of information capitalism has been stimulated by major social transformations, including the increased mobility of populations, the increase of indirect social relations, and the growth of nationwide organizations. This allows for the enhancement of information gathering, the ability to analyse records and the ability to predict future clientele. Kling and Allen refer to the constant pursuit of data-intensive strategies as information entrepreneurialism (Kling and Allen, 1996). This general increase in surveillance, with individuals becoming increasingly monitored and arguably moved, categorized, classified, and validated, increases privacy concerns. Information and knowledge become accumulated, manipulated, and part of a medium of power which

increases with electronic communications and information technology. Governed by others, personal information becomes increasingly important, as such information becomes much more accessible by those that collect it. Within the prison walls, a lot of information is accumulated through observation, but with the panoptic sort, the eyes of surveillance become more difficult to avoid and thus privacy becomes threatened.

The Economics of Surveillance

Economic Origins of the Transformation of Work and Workplace Surveillance

Ranging in use from average sized stores and restaurants to large scale corporations and factories, workplace surveillance has become an important ingredient in the success and functions of any business. From fast food restaurants, such as McDonald's, to large factories such as General Motors, the surveillance of employees, managerial or other, has become a common practice (Garson, 1989; Shaiken, 1984). Surveillance allows management to gather work-related information and evaluate its workers based on such data. Workplace surveillance also allows corporations to counter worker downtime, pinpoint worker inefficiency, increase productivity, maintain an effective, organized and calculated environment, and maintain and increase social control. The surveillance of employees is no longer entirely surprising, since the fact is that surveillance within the workplace is not only common, but has deep historical roots within capitalism and the industrial revolution. As James Beniger argues, previous pre-

capitalistic labour gave way to an intensified, scientifically managed, labour driven, information based, socially controlled, bureaucratized, and rationalized workplace, all of which are sustained and fuelled by intense, almost omnipotent surveillance. The surveillance of employees arose with the birth of the capitalist era, the impact of the control revolution (Beniger, 1986) - which is the social need for the organization and control of information and the eventual exploitation of information - and the emergence of the information society.

The birth of capitalism was not necessarily an easy transition for the common worker. Comfortable in the ways of a self-regulated daily work schedule, workers became pressured into a capitalist system in which they were not entirely comfortable. Dandeker states that "workers were for the most part non-accumulative, non-acquisitive and accustomed to work for subsistence rather than for an incentive based, 'rational' maximization of income" (Dandeker, 1990:178). Since these workers were 'thrown' into capitalism, a system based on increasing the intensity of labour and increasing productivity, modern capitalism faced immense and stubborn resistance from its workers (Weber in Thompson, 1963:356). Thus, there was an increased need for factory discipline and an increasing need for improved managerial control. The worker had to be adapted to the discipline of the machine, creating what Andrew Ure calls a union between capital and science - reducing "the task of his [management's] work-people to the exercise of vigilance and dexterity" (in Thompson, 1963:360).

Max Weber argued that it was necessary to see capitalism as a "moral prescription," a force that bound all members of society, and not necessarily as a desire to

make money (Cuzzort and King, 1989:48). Weber argued that the pursuit of gain, of money, has in itself nothing to do with capitalism, but rather, the spirit of capitalism finds its origins in the rational organization of free labour (Weber, 1963:32). Unlimited greed for gain is not identical to the spirit of capitalism (Weber, 1963:32). However, capitalism is the reinvestment of capital as itself the ultimate purpose of life, rather than indulgence in worldly pleasures (Weber, 1930:53). According to Giddens' interpretation of Weber, Weber is concerned with the rational organization of labour, which means that work is routinized and tabulated, and a capitalist enterprise implies a disciplined labour force and the constant investment of capital (in Giddens, 1930:xi). Weber also argued that there was a calling, a sort of ethical obligation apparently directed toward profit (Weber, 1930:75). But it was not profit and a desire for wealth alone that drove capitalism; instead, Weber argues that through the concept of 'calling', a moral obligation to fulfill daily work in God's grace was provided. But the Protestant 'calling' was not enough to evoke the spirit and morality of capitalism, and Calvinism, where the religious believer is a tool of the divine will and is driven by a doctrine of predestination, became a driving force for capitalism (Cuzzort and King, 1989:50; Weber, 1930:114). A predestined fate, either to be saved by the grace of God or to be ever damned, relegated individuals to a world of uncertainty. But a world of uncertainty does not mean a world without hope, and thus even though material success in life did not guarantee salvation, it was seen as a possible sign of grace - the Calvinist "creates his own conviction, or as would be more correct, the conviction of it" (Weber, 1963:36). Thus, it is the bleakness of damnation and the will of conviction that drove capitalism. As Weber concludes, "one of the

fundamental elements of the spirit of modern capitalism, and not only of that but of all modern culture...[is that a] rational conduct on the basis of the idea of calling, was born...from the spirit of Christian asceticism" (Weber, 1930:180). Therefore, work is given a rational quality, laying the foundations for "capitalistic modes of thought" (Cuzzort and King, 1989:53).

The early need to intensify production "was the driving force behind the establishment of early factories and workshops," as the factory "became a pedagogic institution where...the new standards of conduct and sensibility would be learned" (Zuboff, 1988:31&33). The factory became the breeding ground for workplace surveillance. The gathering of workers in one central location - the centralization of employment - allowed management to intensify control (Braverman, 1975:65). Even before the rise of industrial unionism and social control, Braverman suggests that early forms of workplace domination were found in the 18th century, based on economic, spiritual, moral, and physical forms of domination (Braverman, 1975:67). Shoshanna Zuboff points out that some types of labour discipline involved fines or simply the elimination of a worker or a job. The elimination of one's job became an option with the introduction of steam power which threatened manual labour (Zuboff, 1988). Nonetheless, measures were taken to increase productivity and intensify the labour process. Such a need for discipline within the factory resulted in scientific management.

Taylorism and scientific management allowed productivity to be increased with the streamlining and rationalizing of factory operations (Zuboff, 1988). The scientific management of the workplace by Frederick Taylor, was meant to deal with the rise of

mass production. The scientific management of factories was based on time and motion studies which helped establish work standards and quotas (Marx and Sherizen, 1986:63). Scientific management involved the process of controlling and evaluating the worker, integrating this evaluation with detailed control of production, through "planning and monitoring production by a means of new central management staff" (Lyon, 1994:124). Gary Marx and Sanford Sherizen point out that in "many ways, contemporary monitoring is a continuation of Taylorism" (Marx and Sherizen, 1986:64). However, current workplace monitoring and surveillance in general, has been tremendously enhanced and now focuses not only on the assembly line, but the front office as well (Marx and Sherizen, 1986:64). Taylorism brought to the factory a much needed establishment of management methods, a scientifically oriented organization of labour and a system of social control (Braverman, 1975:85&90). Through the transferring of knowledge from workers, management would be able to eliminate worker decisions and control the actual mode of performance (Braverman, 1975:90). No longer were the workers necessarily responsible for deciding how and when to do certain tasks, but instead, their jobs became fragmented and routinized. The gathering of worker data allowed the creation of a new division of labour and the fragmentation of jobs, while a newly organized management was responsible for the "control mechanisms needed to ensure regularity and intensity of effort while also supplying data" through the reorganization of worker's knowledge (Zuboff, 1988:43). Therefore, Taylorism established a form of surveillance in the workplace that depended on management gathering information regarding specific jobs. The information was then used to establish specific, specialized, and fragmented jobs.

Already specialized tasks became even more specialized, as they were broken down to their simplest component. However, as Graham Sewell points out, information does not constitute knowledge per se, as Taylorism involved "obtaining knowledge [and] proceeded through the gathering and systematic analysis of information...and then through reducing it to empirically derived and universal laws" (Sewell, 1996:788). Sewell argues that the representation of knowledge in its empirical form is extremely difficult, and thus "Taylorism is unable to elicit fully the knowledge exercised by the industrial worker" (Sewell, 1996:788). Workers are still able to incorporate their own personal knowledge and the goal for managers should be to incorporate the new knowledge. Thus, various worker-performed tasks would continuously produce data which would be used by management to reevaluate the monitored tasks.

Taylorism and the move towards capitalism are not the only factors to be held responsible for the current modes of surveillance found within the workplace. Societal transformations and the transformation of work combined social control and the management of information. With the automation of the workplace and the growth of surveillance, information gathering increased enormously. Machines and computers have not only taken the work out of the hands of the worker, and alienated the worker to some extent through the loss of control and autonomy (Wessells, 1990); but also the increase of information generated within the workplace has expanded the web of control. The element of control has been further expanded by the flow of information accumulated by various means of monitoring which included surveillance of not only the employees on the floor, but also the management. This rapid innovation in information and control

technology however, is being used to "regain control of functions [that] once [were] contained at much lower and more diffuse levels of society...[thus constituting] a true revolution in societal control" (Beniger, 1986:7).

Beniger argues that there is a definite relationship between information and control, but it is a relationship that is defined by a "need" for control. All living organisms rely on information and the relationship between information and control, as all organisms order matter and energy (Beniger, 1986:34). Information processing "might be more properly seen as the most natural of functions performed by human technologies, at least in that it is shared by every cell of every living thing on earth" (Beniger, 1986:59). As for society, it must also rely on systems of control, sustaining its organization "against the progressive degrading of [of its own] collective energy" - dealing with the crisis of control (Beniger, 1986:37). The control revolution, at the core of societal transformation dating back to the turn-of-the-century, accounted for "information processing and reciprocal communication, [which were] complementary factors in any form of control" (Beniger, 1986:8). The industrial revolution introduced the crisis of control, but the control revolution "resulted from innovation at a most fundamental level of technology - that of information processing" (Beniger, 1986:9). The crisis of control is nothing more than the disruption of the market equilibrium, brought on by the expansion of markets and the disruption of direct communication due to the industrial revolution. The world was in need of a higher level of organization and communication to accommodate global markets. Thus, Weber's concepts of bureaucratization and rationalization became solutions to the crisis of control, establishing organized systems based on impersonal

relations, the rapid processing of information, the division of labour, and the establishment of hierarchical authority (Beniger, 1986:13-15).

Based on the development of rationalization and bureaucracies, new information-processing and communication technologies arose. Besides the dominant features of bureaucracies, rationalization, and improved technologies, another effect of the control revolution is the emergence of the information society. In response to the ongoing crisis of control, the information society provided the means for the production and distribution of knowledge (Machlup in Beniger, 1986:21). The information society increased the speed and flow of information that began more than a century ago. Computing technology does not "represent a new force only recently unleashed on an unprepared society but merely the most recent installment in the continuing development of the control revolution" (Beniger, 1986:435).

The crisis of control, generated by the industrial revolution and the expansion of the global market, gave way to a social system of control based on the manipulation of information. The "Control Revolution", a series of rapid changes "in technological and economic arrangements by which information is collected, stored, processed, and communicated," marks a dramatic leap from the industrial revolution which harnessed energy, to a revolution based on the exploitation of information (Beniger, 1986:434). It is this cybernetic need for control and the establishment of an information society, that directs us towards the need for surveillance, and in particular, workplace surveillance. There is a need to organize the work environment, in order to accommodate and initiate the flow and control of information. The control revolution is not necessarily only a form

of social control, but a form of social organization; a system that involves the gathering and processing of information on a global level and on a local level, including within the workplace. It consists of the coordination of societal components, maintained by a system of communication and the process and flow of information (Beniger, 1986).

Chapter 3 - Working for the Camera: Surveillance and the Workplace

Monitoring and Surveillance in the Workplace

*To be or Not to be Monitored, That is **Not** the Question*

It should no longer be a surprise that our daily activities, inside and outside the home, are being monitored and information about us is being stored. We are not necessarily part of an Orwellian society, where a degree of social trust has broken down and an element of violent coercion exists, but we do have the tools and the means to implement such a state (Perrolle, 1996:59). We are also not part of a society where we are constantly being watched every second of the day, no matter where we are, although this can be accomplished technologically. Total paranoia, inspired by the possibility of an Orwellian state, is partially but not entirely warranted. However, what needs to be understood is that although we are not *always* being watched, we are *increasingly* susceptible to being watched, by both suspecting and unsuspecting eyes within the workplace. We may in fact be constantly monitored, but not always in a focussed manner (Lyon, 1994). We have fewer places to hide and an even harder time protecting our personal information from electronic eyes and from those who collect and store it (Lyon, 1994). Our daily activities reveal information that can be both helpful and detrimental towards our past, present, and future. A simple online conversation, a quick transaction at the local store, and more importantly, a routine day at the office become informational

reference points. Our daily activities can be digitally reduced to binary codes, stored in bytes, and retrieved in split seconds. Face-to-face personal interaction is replaced with signals, symbols, beeps, and modem screeches. The retooling of relationships within the workplace, created by the increasing ease of communication, creates new interpersonal relationships and alters existing ones, doing away with the familiar formal and informal relations (Perrolle, 1996). Knowingly or unknowingly the information we continually emit, inside and outside the workplace, contributes to a self-made, technologically generated, and objectified persona. This persona is dissected by those who control and evaluate the information. But what makes this technological relationship between the watchers and the watched, and, in particular, the employer and the employee important, is the degree to which the relationship has been altered, especially in the workplace. The relationship between employer and employee has been intensified, enhanced, and threatened all at the same time.

The workplace has historically been an area where monitoring and surveillance have been combined, with discipline and constant improvements in worker productivity being the main focus. Taylorism and scientific management were not meant to improve worker relations, but were meant to increase labour power, to increase individual productivity, and to establish a disciplined workplace where constant monitoring was a possibility. As Braverman points out, Taylorism is not a "science of work [but rather a] science of management of other's work under capitalist conditions" (in Hecker and Kaplan, 1989:698). With the push towards increasing production, constant surveillance and monitoring were meant to assure productivity and counter laziness. The workplace

has also become a battleground for the re-negotiation of employer/employee relations. According to Judith Perrolle, the question of privacy and worker solidarity has to be re-evaluated in the workplace in light of new forms of technology and the reification process, "the embodiment of social relationships in objects" (Perrolle, 1996:55). Privacy in the workplace needs to be addressed in terms of how much privacy should be ensured without isolating the employee, as well as how privacy can be established while maintaining a mutually beneficial relationship between employer and employee. Other privacy concerns include the preservation of the integrity of different forms of communication, the preservation of formal and informal relations, and the extent to which so-called private information becomes company property. The issues are not only why monitoring and surveillance occur, how they occur or where they occur, but also what surveillance and monitoring provide the employer and the employee, how employer/employee relations are affected, what the bounds of surveillance are, what the defences against workplace intrusion are, legally and otherwise, and the implications of all this for privacy.

Monitoring, Surveillance, and Databases - What Does it all Mean?

The terms "monitoring" and "surveillance" have been used interchangeably at times. They are however interlocking terms with distinct differences that complement each other rather than assume each other's meaning. Monitoring is the act of watching and listening over others, either by being directly in the same space or close by.

Alternatively, monitoring can be "undertaken remotely in space," with the help of computers, enhanced visual devices, satellite imaging and positioning and infrared devices (Clarke, 1988:499). Surveillance, on the other hand, enhances the process of monitoring by adding a degree of supervision for specific purposes and the collection of information (Lyon and Zureik, 1996:3). Its primary purpose is "generally to collect information about them, their activities, or their associates;" ("them" refers to those that are being watched) (Clarke, 1988:499). The key difference between monitoring and surveillance is that surveillance uses and collects the information produced by monitoring in different social environments, such as the workplace. Surveillance also uses the information in different social contexts for means of social control - the shaping of behaviour and ensuring compliance with social and workplace norms (Mowshowitz, 1996:79). James Rule and Peter Brantley define surveillance as the "monitoring of human behaviour, with an eye [on] enforcing the expectations of those in charge." (Rule and Brantley, 1992:406).

With the accumulated information, employers can create massive databases on their employees, generating a databank system made of personnel files, each containing personal employee information which may or may not be work related. As Roger Clarke explains, the accumulation and storage of massive amounts of information can lead to "dataveillance," or the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988:499). Workplace surveillance is not merely the recording of personal biographic information of an employee, but it also includes the monitoring of an individual's work habits,

productivity levels, and expenditure of time, as well as personal habits, personal communications, and "off-the-clock" activities within and even outside the confines of the work environment. Employees become data subjects; impersonal data sets which become identified numerically or electronically. In accordance with mass surveillance, Clarke states that personal dataveillance is concerned with identifying individuals who might be considered suspicious; a useful tactic for the employer who is suspicious about one or more employees (Clarke, 1988).

The surveillance of an employee is not only a concern because of its potential invasion of employee privacy, but also because there are many uses for the information retrieved. As Andrew Clement points out, with the implementation of surveillance and databases in the workplace, and the creation of personnel databases, "these fine-grained profiles of individual employee behaviour...can be used in situations far from what was originally expected," (in Cavoukian and Tapscott, 1995:117) thus creating, according to Clement, a "fishbowl" workplace. Clement argues that our daily work activities and lives become transparent, with the further threat of that transparency moving beyond the walls of the work environment. Different than the sweatshop, Clement argues that although fishbowl surveillance is less visible, a wider range of employees are affected (Clement, 1992:25). "The pursuit of control over all relevant aspects of the business enterprise," signifies a logical extension of the central management paradigm and the implementation of a workplace panoptic principle (Clement, 1992:26). Herein lies the threat and the problem. A distinction must be made between private and public information, or better yet, useful and useless information, within the confines of the workplace. Private

information in this case is considered employee information that is not specifically work related. An employer needs to make a distinction between what is necessary and what is unnecessary information. The problem, however, is that distinguishing information does little good when management can potentially use all forms of information gathered. Personal information and employee work habit information can both be used in increasing workplace efficiency. Social control, or better yet, employee social control, can increase with the intensive collection of information *only* if the employer *uses* that information. What must also be understood is that the collection alone of information does not signify the use of that information. We must also be aware of the potential use and misuse of such information. Thus, the focus is not necessarily only on the distinction between private and public information, but on what the information be used for.

From a government perspective, the Canadian government is being pressured to establish laws to distinguish and establish boundaries limiting surveillance in the workplace without totally curtailing it. However, in spite of the attempt to subdue workplace surveillance, which is both beneficial and hurtful to employees, there is no need to totally remove the teeth of surveillance, just lessen the bite. Also, employees and unions must decide how an employer may use certain monitoring techniques, and to what extent surveillance and the collection of information can be exploited and curtailed at the same time. Surveillance in the workplace is not inherently bad, but the abuse of surveillance can be detrimental to both the employer and employee. Employees who feel that their rights have been infringed upon might become aggravated with management and attempt to resist certain forms of surveillance, which benefits neither party. Increased

levels of stress, the lowering of employee morale and unproductive work cycles are some of the consequences of intense workplace surveillance. However, the employer benefits from the surveillance of employees because a wide range of information can be collected and used towards the rationalization and control of production. For example, data collected through surveillance can result in modifying various work areas or even help shift onto the employee various costs that management had initially to absorb.[5] The employee can potentially benefit because they can receive positive feedback from management with regards to their work performance. But what still needs to be determined is how surveillance and the collection of information in the workplace becomes a mediator in employee/employer relations. The relationship between the employer and employee becomes not only a legal problem, or only an economic, rationalized calculation, but also a social relation, a relation that involves trust, privacy, and awareness. It is this social relation, found within the panoptic workplace, that becomes a concern. Also, it is important to note the notion of self-discipline within the walls of the work cubicle.

---

[5] This example refers to a case that happened at Hershey Foods Corporation. Data collected from employees identified costly benefits that could be reduced, as health records listed those who had higher medical risks and thus health insurance premiums were passed onto the worker based on their specific health file (Staples, 1997:115). Those who refused to take, what were referred to as "wellness" tests, were automatically charged the highest premium. The company responded by saying that "now we need to evaluate the people with something to hide" (in Staples, 1997:115).

Spies Like Us - All from the Comfort of Your Chair

Who is Doing the Watching, At What Financial Cost, and Why?

No longer is the question *"is* somebody watching us?," but *"who* is watching us?" Although statistics vary, workplace surveillance is definitely on the rise. Inspired by a need for increased productivity, greater organization, the rise of the disciplinary society, and most importantly the measurement and appropriation of employee knowledge, there has been a "fundamental need for capitalist control of labor power" (Sewell, 1996:788; Hecker and Kaplan, 1989:695). Based on Foucault's interpretation of the Panopticon, Marx's distinction between labour power and labour, Taylorism and scientific management, and the fundamental need for the capitalist control of labour, several companies have adopted workplace surveillance (Hecker and Kaplan, 1989:695). The monitoring of employees has increased and has also been modified, moving beyond the art of calculating individual daily production levels to the more intensive minute-by-minute evaluation of a worker's day. The art of surveillance has been intensified to the point that not only are the watched being monitored, but the watchers are also being monitored by their supervisors, and to some degree by the workers themselves - thereby producing a multi-flowing, bi-directional, hierarchy of surveillance. Who is watching whom and when?

In the United States, many Fortune 500 companies have invested millions of dollars in internal and external security measures. According to one of the largest and

oldest associations for security professionals, the American Society for Industrial Security (ASIS), more than half of their customers, which are typically Fortune 500 companies, spend between US$100,000 to $5 million per year on security (Whalen, 1995:1). Most of the money goes towards access-control systems, systems which require a certain level of security clearance, are password protected, and use CCTV surveillance. Another study states that the use electronic monitoring in the office has doubled from approximately 20% of businesses monitoring their employees in 1984 to about 40% more recently [1993] (Aiello, 1993:499-500). A more recent study (1997) found that 35% of employers use one or more types of "close" electronic monitoring on their employees and 63% of them use less invasive kinds of electronic monitoring (Brin, 1998:56). And finally, a 1998 *Info World* magazine study found that 76% of the executives surveyed monitored employee Internet usage, while the same study found that only 54% of the employees knew that they were being monitored in some capacity (1999:61).

Comparable Canadian studies on workplace surveillance have not been done, but there are signs that the numbers are consistent with the U.S. Grant and Higgins (1991) found that 35% of service-sector clerks were subject to some form of monitoring while the Ontario Federation of Labour "reports that a survey of conference attendees showed 20% of its members experiencing electronic surveillance," while this number rises to 38% for government and crown corporations (in Clement, 1992:23)[6].

Big businesses are not afraid to implement surveillance devices in the workplace,

---

[6] Granted these numbers are dated, with the latter statistics being in 1985, but it is unlikely that these numbers have decreased, and probably have increased in the last 15 years.

keeping close tabs on their employees in hopes of cutting down on "offenders" caught wasting company time and resources. Even high profile companies such as CNN, a subsidiary of the Turner Broadcasting Corporation, use surveillance cameras, hidden cameras, and swipe cards for more than mere security measures. Alan Deniro, the human resource manager of Turner Broadcasting, admits that such devices record and track employees, and that the employees have been told that their voice mail, e-mail, phones, files, Internet travels, and desk drawers are all prone to be monitored and searched. Deniro claims that "when the day is done, those (devices of communication) are company property and as company property, the company reserves the right to, in some way and in some instances, go in and investigate [their] use" (Interviewed on CNN Impact, 1997). It is an exchange of privacy for a pay cheque - a relationship that binds the employee to the workplace and is a crucial aspect of the employer/employee and workplace/privacy/ employee relationships.

Monitoring in the workplace, however, comes with a financial price. US statistics show that, "between 1990 and 1992, more than $500 million was spent on surveillance software by more than 70,000 US companies," with expenditures estimated to rise considerably, hitting the billion dollar mark by 1996 and even more by 2000 (Aiello, 1993:500). An increase in security expenditures means that more and more workers are being monitored, with more advanced technology. The Office of Technology Assessment of the US Congress estimated that more than 10 million US workers would be monitored by the year 1990, a number which has surely risen in the last nine years (Aiello, 1993:500). *Macworld* magazine's survey found that in 1993, "as many as 20 million

Americans may be subject to electronic monitoring through their computers (not including telephones) on the job" (Whelan, 1995:4). More than 20 percent of American employers admitted to engaging in some type of surveillance, with the vast majority claiming that electronic work files are searched and 40 percent claiming that e-mail accounts are investigated.

Why companies are putting so much emphasis on surveillance in the workplace is a complicated issue. Despite the historical arguments, the need for worker discipline and the effects of capitalism, some of the common and more specific reasons for workplace surveillance have to do with the issue of trust. First of all, companies stress that there is a growing level of mistrust aimed at employees. One of the more "favourite" statistics cited is that "eighty to ninety percent of...business theft is internal" and 29.2 percent of respondents gave this as a reason for monitoring work (Whelan, 1995:2; International Labour Office, 1993a:25). Other issues of mistrust have to do with employees stealing company time for personal reasons, as well as stealing and then sharing company ideas with competitors (Whelan, 1995:2; International Labour Office, 1993a:25). Stealing company time is a major issue among the bigger and middle sized corporations, which can lead these corporations to the constant tracking of employees. Monitoring which doors employees use and how long employees are in certain areas becomes common practice.

Another popular fact is that corporations are worried about computer-data trashing and "other economic sabotage [which] is on the rise because of employee resentment in the era of corporate 'downsizing'" (Whelan, 1995:2). Almost 22 percent of respondents

employed in large US corporations gave espionage as the main reason for monitoring workers (International Labour Office, 1993a:25). When public relations can not soothe the disgruntled employee, there is always the threat that the employee may retaliate. One corporate businessman stated that "there are 2 million schizophrenic people in this country [the US]...not everyone is extreme, but you've got to be prepared" (Whelan, 1995:2). Finally, more and more companies, particularly in the US, are turning to monitoring devices "to increase their control over employee behaviour and improve internal security" (Marx and Sherizen, 1986:72). These reasons seem to argue that surveillance in the workplace is done not only to improve productivity, but also out of fear. Surveillance in the workplace has gone beyond the notion of curbing deviant behaviour to creating an arena of self-discipline, while attempting to predict and eliminate problems before they even happen. The grave concern of company owners, management and investors over the impact of worker negligence, mistrust and theft, forces companies to react by installing monitoring devices.

Complete surveillance, however, does not guarantee complete compliance. Richard Rosenberg points out that the "endpoint of all technology is to increase productivity, [but] the creation of an environment where all activities are monitored surely stands to defeat this purpose," because productivity might suffer due to an increasingly uncomfortable working environment (Interview with Rosenberg on the CBC, The National Magazine, 1998). Face-to-face surveillance has been done for centuries, but with the ability to go beyond such a relationship, with in-depth searches, intensive information retrieval, and the recording and dissemination of information which can be

done from anywhere and everywhere, the employer-employee relationship and the issue of privacy become redefined. Replacing face-to-face surveillance with technological surveillance capabilities alters the relationship by creating a disciplined and self-disciplined environment which increasingly threatens privacy, and diverts attention from the initial rationale of bureaucratic organization meant to increase productivity. Surveillance can become an external threat manifested internally, pressuring employees, increasing levels of stress, and hampering rather than promoting consistent, productive work. Electronic monitoring in the workplace "raises problems that differ from more conventional forms of monitoring [because] much of the concern involves the radical changes in the nature of the monitoring, which can involve secrecy, continuous monitoring of every act and movement, and a variety of consequences on working conditions and health of workers" (International Labour Office, 1993a:11).

In contrast, some suggest that there has been a slight exaggeration of the panoptic effects of surveillance. Matti Pringle and Paul Edwards claim that not all workers accept passively the effect of the 'Electronic Panopticon' (Pringle and Edwards, 1995). Rather than workers becoming robots, they can be better described as 'donkeys' - "individualised and largely powerless employees who none the less manage to find ways to make life tolerable and to blunt the sharpest edges of managerial control" (Pringle and Edwards, 1995:I). Some employees constantly dupe the system, by rushing jobs and cutting corners to find some free time on the job, thus providing room to resist. For example, travel agents at major U.S. airlines are able to find loopholes in their employee monitoring system. By keeping customers on the phone for longer periods of time while inputting

data, the intended break between calls meant for data input is reduced to seconds instead of minutes, allowing for additional breaks every few hours (DeTienne, 1993:34). Pringle and Edwards argue that electronic surveillance is important merely as "a new weapon in management's means of control and not a qualitative leap" (Pringle and Edwards, 1995:28). It is how management uses surveillance technology to its fullest extent that will intensify bureaucratic control. But claiming that an employee can beat the system, does not diminish the panoptic capabilities of workplace surveillance. The attempt alone to dupe the system is essentially the problem. The *need* for an employee to "outsmart" any form of monitoring is a problem on its own. Pringle and Edwards fail to account for the reasons behind employees' attempts to dupe surveillance methods.

Although currently at all levels of work the panoptic function is not fully employed, the potential to limit worker's autonomy and create a more totalising work environment is attainable. With direct means of control within the workplace, productivity becomes a major concern for management. However, the discussion of surveillance has instead become a discussion about privacy, with employee human rights becoming a common ground for anti-surveillance arguments. The debate over privacy, although an important one, can be a misguided one, if all of the factors regarding surveillance in the workplace are not considered.

This essay is based on the assumption that the surveillance and monitoring of workers is detrimental to the welfare, the legal rights (ie. privacy rights), the economics (ie. productivity), the social relations, and the privacy of employees. However, this assumption is not presented carelessly as several studies demonstrate the negative effects

of workplace monitoring. The assumption that monitoring in the workplace is detrimental to productivity, and more importantly, an invasion of employee privacy is not only based on anecdotal and political cliches, although the tendency to do so is not uncommon, but also, as I endeavour to show, empirical studies have shown that monitoring in the workplace do provide a negative environment for employees.

Surveillance in the workplace is not always accompanied by negative consequences but rather employees are able to deal with the technological engineering of the work environment. Delbert Nebeker and B. Charles Tatum (1993) argue that, based on their studies, some contrary claims against opponents of computer monitoring can be made. They argue that no negative effects associated with "the computerized recording, analysing, and reporting of performance on database operators," were found (Nebeker and Tatum, 1993:532). Employees that received performance feedback and were aware that their performances were being monitored had a boost in key rates without sacrificing quality, increasing stress or reducing satisfaction (Nebeker and Tatum, 1993:533). Nebeker and Tatum also concluded that if worker standards were in line with employee self-perception and there were reward incentives for meeting certain goals, then computer monitoring would be more readily accepted (Nebeker and Tatum, 1993:533). If employee goals could be reached, then employee satisfaction would be high and there would be little concern among employees regarding the monitoring of their work production. Nebeker and Tatum thus conclude that a happy medium between employee monitoring and job satisfaction, levels of stress, and adequate levels of productivity can be reached.

Other studies however, have shown that monitoring does have negative effects on

employees. Bob Baldwin, the national director of social and economic policy with the Canadian Labour Congress, claims that the workplace is more stressful than ever now with intensified surveillance (in Menezes, 1999:11). Baldwin makes this claim, based on union research, that "staff monitoring is usually related to unrealistic performance expectations on the part of employers" (in Menezes, 1999:11). Phillipa Lawson endorses Baldwin's claim by suggesting that monitoring employee e-mail could have "a very demoralizing effect" (in Menezes, 1999:12), while Canada's Privacy Commissioner, Bruce Philips, states that "with each new form of surveillance, we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for 'corrective measures'" (in Arnaut, 1996:C1).

Specific studies done on workplace monitoring support Lawson, Phillips, and Baldwin's claims. Elia Zureik and Vincent Mosco's study on the general impact of technological change on the labour force in the telephone industry, pointed out some of the effects of employee monitoring. The various telephone employees experienced a multitude of effects when it came to performance monitoring. Some employees experienced increased frustration due to the fact that they felt they were being spied upon, others felt increased levels of stress and a lack of control over their work, some operators felt that they had virtually no control over the pace of their work, while others telephone company employees felt that the competition between co-workers increased because of the need to keep up one's work "statistics" (Zureik, Mosco and Lochhead, 1987:75-82). Out of all the different types of workers found in the telephone industry examined, an

average 67.79% of the workers claimed that monitoring was a problem, and many workers felt "stress as a result of pressure from management to be productive [and] reduce absenteeism" (Cruickshank, 1987:62, Zureik, Mosco and Lochhead, 1987:78). Similar results were found by W.S. Brown who noted that studies have linked "psychological illnesses such as anxiety, depression and nervous breakdowns to the stress induced by continuous computer monitoring of workplace performance (in Fairweather, 1999:43). C. Fried argues that information collected by employers may lead subjects to be more apprehensive and inhibited because the information might fall into the wrong hands. Fried's argument suggests that it is not the monitoring itself that is only problematic, but what happens to the information after it is collected becomes a concern as "there is always an unseen audience, which is more threatening because of the possibility that one may forget about it and let down his guard, as one would not with a visible audience" (in Fairweather, 1999:43-44). For Fried, the threat in the workplace has more to do with impression management[7] than actual intrusion. The employee is

---

[7] I am using Erving Goffman's term of impression management in this example (Goffman, 1959). Impression management occurs when an individual is involved in staging a character. In this case, it would be the employee who is forced to stage the character of the 'perfect' employee. The employee could be putting on a performance for management, concealing, what Goffman calls, inappropriate pleasures - the hiding of other activities which are inappropriate for the role, but not necessarily inappropriate in general (Goffman, 1959:43). We could also use Goffman's concept of the role which consists of "the activity the incumbent would engage in were he to act solely in terms of the demands upon someone in his position" (Goffman, 1961:85). Goffman's role concept is one that involves face-to-face interaction, but the idea that an individual must keep command of himself or herself within the workplace, even without face-to-face interaction or surveillance, is still relevant. Finally, the concept of role distance can also be applied to the role of the employee. Role distance is the "expressed pointed separateness between the individual and his putative role" (Goffman, 1961:108). Goffman explains that role distance involves the denial of the virtual self implied in the

responsible to "act" appropriately, to act like the diligent worker he was hired to be. R.C. Manning focuses on the issues of intrusion and trust, claiming that the "sharing of information is merely a consequence of trust and caring which is part of intimate relationships" (in Fairweather, 1999:44). However, Manning argues that this does not make monitoring less serious as surveillance eliminates the relation of trust between employer and employee, thus diminishing employee self worth. Finally, an international study by Michelle Jankanish (1994), which was conducted in 19 industrialized countries, found that "electronic monitoring can create adverse working conditions that lead to stress, extreme anxiety, depression, anger, and severe fatigue" (Arnaut, 1996:C1).

Shoshanna Zuboff also found elements of "vulnerability and powerlessness due to a new visibility of the informated workplace" (in Brown, 1996:1242). Zuboff claims that this unknown, relentless exposure leads to mistrust but that this mistrust is not "rooted in a perception of evil or malicious intent" (Zuboff, 1988:344). Finally, Clement boldly states that recent Canadian experiences do not concur with various studies on surveillance in the workplace where it is argued that "computerized monitoring could provide a valuable ingredient for the democratic operation of modern, thoroughly computerized enterprises" (Clement, 1992:41). Clement argues that "experience with electronic surveillance in Canada over the past decade does not offer grounds for optimism that [Zuboff's positive vision] will soon prove to be the norm" (Clement, 1992:41). Granted Clement's final statement is a critical one, eliminating any potential for the positive aspects of workplace surveillance, such a statement should make one aware of the

---

role, not the role itself (Goffman, 1961:108).

potential consequences of intense workplace monitoring.

The Eyes of the Foreman vs The Infrared Beam

Employee drug tests, urinalysis, medical records such as HIV tests and genetic screening, video surveillance, visual observation either by the physical presence of a manager or through an inconspicuous two-way mirror, lie detector tests, e-mail monitoring, psychological tests, wiretapping, infrared badge monitoring, voice mail monitoring, and keyboard stroke recording are several of the possible methods of surveillance that employers use to track their employees. Each method provides a specific type of information, yet all follow a similar objective, that is the accumulation of employee information. The methods of genetic screening and monitoring, e-mail monitoring, and video surveillance will be specifically focussed on below, because they provide three slightly different types of surveillance and different types of invasion of privacy.

Genetic screening and monitoring suggests that surveillance has progressed to a form of prediction rather than relying on current information. Genetic screening allows an employer to make assumptions about certain employee's future performance. Video surveillance, on the other hand, depending on where and when it is used, can be considered, by some, as a much needed control device or, by others, as a severe invasion of privacy. Video cameras rely on instantaneous video images, which can be taped, saved and stored. They also possess the ability to be in constant or random use, which creates

the problem of unsuspecting violations of privacy. Video surveillance differs from the traditional episodic monitoring by the supervisor (Marx and Sherizen, 1986:65). Finally, the monitoring of e-mail creates a new problem in terms of distinguishing what is public and what is private information. Electronic mail is at the centre of a large debate, mainly because there are no laws protecting an employee's electronic mailbox and yet there is the assumption that e-mail is private. The focus on these particular surveillance practices does not suggest that they are of greater importance than other methods, but rather, that these three methods have become increasingly more common over the last ten years. They provide information which can potentially threaten the notion of privacy in the workplace. However, a brief discussion of several surveillance methods in the workplace is necessary to demonstrate the scope of surveillance and the degrees of privacy invasion.

Drugs, Lies, and Videotapes

Drug Tests

Testing employees for the use of drugs is not a new policy, but one that has been implemented by employers and fought against by employees and unions for some time. Under the assumption that there has been an upsurge in drug use especially in the US, companies have adopted a highly contentious stand by claiming that they have been "eager to take up the [drug] cause, focussing on the productivity and safety problems connected with substance abuse and their alleged major contribution to the loss of

'competitiveness' of American industry" (Hecker and Kaplan, 1989:702). A 1992 US study showed that over 25% of Fortune 500 companies performed random urinalysis on potential job applicants and sometimes current employees (DeCew, 1994:18). Both government and private employers argue that there is a serious need to conduct drug tests to insure workplace safety; to identify those who would be unable to work in the future; to reduce the costs of employee health plans and "to maintain public confidence in the integrity and trustworthiness of their (the companies) operations" (DeCew, 17:1994). Employers have taken measures against drug use, illegal or legal in the case of alcohol, by forcing employees to take random urinalyses tests. Some estimate that US$1.2 billion was spent on drug testing in 1992 in the US alone (Brin, 1998:56). Studies have shown a correlation between crime and drug abuse and thus the mentality that "increasing or reducing the level of drug abuse is associated with a corresponding increase or reduction in criminality," which "may have provided the earliest theoretical justification for initiating drug testing programs" (DeCew, 1994:17-18).

Despite an increase in the general abuse of drugs, workplace drug tests, to some degree, are misguided. Steven Heckler and Mark Kaplan, argue that even though there are significant production costs related to employee drug use, alcohol is responsible "for more than twice the costs in lost productivity and treatment," compared to illegal drugs which are focussed upon in drug tests (Hecker and Kaplan, 1989:702). Thus, drug tests are useful but not totally effective in terms of deterring low employee productivity and ensuring safety in the workplace. Drug tests have also been criticized for not being able to accurately monitor a worker's performance. A 1993 document by Tom Wright, the

former Information and Privacy Commissioner of Ontario, found that "random drug testing does not have the capacity to monitor the use of drugs or alcohol in the workplace, nor is it capable of indicating the effects of drug or alcohol use on a worker's performance...rather, the testing can show only that drugs or alcohol had been consumed at some time in the period before the test was applied" (Wright, 1993). There have been several times that drug tests have failed to "show a convincing and general link between accidents and drug use" (Gilliom, 1994:41)[8]. Drug tests also have been known to have a 40% to 60% failure rate and the tests detect not only illicit drugs, but also legitimate drugs (Cavoukian and Tapscott, 1995:121; DeCew, 1994:18). A relatively high failure rate, the potential to misinterpret drug tests, and the limitations of drug testing are some of the reasons why there are so many opponents of it.

In addition to such shortcomings, there is also a more crucial problem with drug tests which has to do with the invasion of privacy. Drug tests invade a worker's privacy on several levels. One major concern is the "technological and physical intrusiveness into a person's biological functions in the actual procedures used for collecting samples" (DeCew, 1994:18). An employee might have to be subjected to the intrusion of a needle for blood tests or a urine test done under direct supervision, creating an uncomfortable environment for the employee (DeCew, 1994:18). Furthermore, drug tests not only reveal what an employer is searching for, i.e the abuse of drugs, but "besides confirming or disconfirming the presence of drugs in the body, analysis...may reveal numerous...facts,"

---

[8] Gilliom points out the following cases where drug tests have failed to link accidents to drug tests: Zwerling, Ryan and Orav, 1990; Federal Rail Administration, 1988 (Gilliom, 1994:41).

that the employee may not wish to be revealed (DeCew, 1994:18). Tests can reveal if an individual is using contraceptives, is pregnant or is suffering from a particular disease. These pieces of unnecessary information, which are unavoidable, cause even more concern over privacy. Drug tests question a worker's daily habits outside the workplace, threatening an employee's privacy on a different level. The employee now has to worry about what he is doing both during and outside office hours. The monitoring of employees outside of the office means that an employee is either physically outside of the work environment or else a worker is 'off the clock', but within the physical work environment.

Drug tests can invade an employee's privacy in present time and historically, as drug tests can invade one's recent past in an attempt to find incriminating information. Drug tests can also create a level of mistrust amongst employees as well as a strain between the employer and employee. Some analysts argue that drug tests may be counterproductive because they can "misidentify problems, alienate workers, and deplete resources from other policies" (Gilliom, 1994:36). With regards to drug tests and other methods of surveillance, one of the main legal concerns is the ability to determine "when the interests of others are significant enough to outweigh the threats to test subjects and when the achievable goals outweigh the negative consequences of testing" (DeCew, 1994:21). At the same time however, it must also be noted that drug testing, as well as other surveillance methods, must be placed in "the broader social context of fundamental changes in the organization of control" (Gilliom, 1994:37). Workplace safety and productivity become an aspect of workplace control, as the enforcement of norms through

surveillance increases in companies (Gilliom, 1994:37).

Infrared Badges and Active Badges

The creation of the new "media spaces", as Anne Cavoukian and Don Tapscott point out, eliminates the need for the supervisor to be in the employee's immediate space (Cavoukian and Tapscott, 1995:124) Multimedia technology allows for the employee to be followed and glanced at periodically from any location. Active badges, similar to the concept of the controversial smart cards, can track and locate employees as well as record where employees have gone during the day or any other period of time. More sophisticated devices, such as the Bellcore Cruiser and the Xerox Europarc Rave, "offer services ranging from complete two-way video/audio connections lasting an indefinite time...to brief connections only a few seconds long" (Cavoukian and Tapscott, 1995:125). Devices such as infrared badges emit infrared beams to sensors located around the office. These devices can emit constant or periodic signals and can be recorded from up to eight feet away. These badges also provide timing information, recording the length of time an individual spends in one location, say at one's desk or in the washroom.

These badges are an infringement of privacy on several levels. First of all, the badge adds an Orwellian atmosphere to the workplace, as the badge must be carried around at all times (Cavoukian and Tapscott, 1995:124-125). Secondly, the distinction between public and private information becomes blurred, as the badge is unable to distinguish when the wearer is in a private or public location, regardless of whether or not

the individual is on official company time. Finally, the badge removes a sense of control from the employee, as it is the employer or the controller who is able to remotely record the information. However, there have been strides towards returning some control and privacy back to the employee by equipping the badges with a type of security device that notifies the wearer that they are being detected or that someone is approaching them. By erecting these electronic barriers, "privacy 'doors' may be closed or slightly left ajar" (Cavoukian and Tapscott, 1995:125). Concerns regarding the ability to control the information exposed to the badge, however, are never ending.

Electronic Mail (E-mail)

Continuously gaining in popularity, electronic mail, or e-mail, has rapidly established itself in the business world as well as in the public domain. Based on the concept of being able to send messages and files from one computer to another with the touch of a key, e-mail has allowed users to partake in quiet, almost effortless, conversations. Geographical distance becomes a concern of the past, as e-mail unpredictably flies through cyberspace, taking random paths, travelling across the world or across the office, in seconds. E-mail allows individuals to contact virtually anybody, from anywhere in a virtual world. From the comfort of one's office cubicle, a user is linked to the world with the ability to e-mail millions of people.

However, the simplicity and ease of e-mail has raised some serious questions with regards to the privacy of the paperless communication. E-mail does not travel a

necessarily secure or safe route. Information from one computer to another can be intercepted at any time, at any point. Information that can be sent in a split second can be intercepted just as fast, threatening the privacy of the sender and the recipient involved in the e-mail transaction. As Tom Wright points out, one data security expert has claimed that e-mail has "the same security level as a postcard" (Information and Privacy Commissioner, 1994:1). Not only can e-mail be intercepted, but it can be traced, stored, retrieved, and is deceptively hard to destroy. This easy access allows external parties the opportunity to monitor e-mail, a potential violation of privacy that has many employees and unions concerned.

The fact that e-mail is so accessible by both its user and external parties, lacks legal protection, and is not easily defined in terms of ownership, consequently threatens the privacy rights of employees. Technology has provided us with a paperless, silent method of communication, which ironically screams for protection. Without the physical evidence of the transaction of information, it becomes difficult to determine exactly what, and who needs to be protected. Particularly in the workplace, the issue of e-mail has raised some complex legal and ethical questions regarding the right to privacy of e-mail users (Wright, 1994:1). The ease of passing information has allowed for the ease of monitoring the information.

Although e-mail has facilitated communications, it comes with a price which many may not want to pay. The problem with e-mail, and computer files in general, is that literally anyone can access them, even after they have been supposedly deleted. Employees might think they have deleted certain e-mail files, but "the scary, interesting

thing about computer files is just how much they proliferate and how long they linger, and the lack of control people have other them...they are ephemeral in many ways...but they're more permanent than people might want to think" (Lind, 1998:IT11). Essentially, "any skilled person can recover the message's ghost somewhere deep in the bowels of a networked system," which raises some serious concerns about employee privacy (Plummer,1998). Employers can monitor and search through e-mail messages sent days, weeks or months ago in hopes of finding incriminating information, or simply performing routine checks. The practice of employers monitoring e-mail is not uncommon. According to the American Management Association, nearly two-thirds of businesses surveyed claimed to monitor e-mail or "use other methods to electronically eavesdrop on their workers" (Plummer, 1998).

But is the monitoring of e-mail messages necessarily an invasion of privacy? The information sent by e-mail could be private personal information, but that is exactly why employers need and want to know if private information is being sent during company time. If personal information is being sent on company time, it is a potential waste of that time and damages productivity. Businesses argue that if they want to protect their companies and focus on increasing productivity, there should be a limit or a total ban on personal e-mail. Also, if such e-mail can be costly for the employer or business, for example by distributing company secrets, the business should be able to intervene and stop an employee from doing so. But what is company time? Dave Banisar argues that "employers are demanding more from us by equipping us with pagers and requiring us to read e-mail at home," and thus should be more accommodating to employees privacy

rights (in Plummer, 1998). If employers are giving us the technology to communicate, and demanding more of our time, why should employees not be able to privately use the technology on their free time? Even e-mail sent during one's break are open to scrutiny by employers.

Besides the violation of wasting company time, employers also argue that they have a certain proprietary right which warrants monitoring an employee's e-mail. Businesses argue that since they provide the means to send e-mail, they own the rights to the machines and the messages being sent. Although there have been no current cases in Canada regarding e-mail privacy in the workplace, US cases "have consistently found that if the employer owns the machine, it owns the information inside the machine as well, and even an employee's personal correspondence" (Fitz-James, 1999:E4). Once an employee logs on to the network, every message sent and received becomes company property. If the company owns the property and the e-mail message, then they have every right to read, store, and retrieve employee e-mail. Owning company e-mail and computer files, however, can also become extremely damaging for businesses, because any sort of criminal activity done through e-mail can then be traced back to the employer, who owns the means of communication. Thus, businesses are warned that if they are monitoring e-mail, they should institute 'technical equipment use policies' "to make it easier to discipline or fire employees who misuse company equipment, and to reduce the company's exposure to lawsuits or criminal charges" (Fitz-James, 1999:E4).

E-mail is thus a double edged sword. It can improve communications, even flatten "traditional hierarchical structure(s) of an organization by breaking down barriers to

communication between employees and their employers and managers"(Wright, 1994:4). Yet, it can also create a hostile environment where employees begin to fear their privacy is being invaded, thus adding stress and anxiety to an already hectic workplace (Wright, 1994:4). Amitai Etzioni goes as far as to say that by using e-mail spot checks, "employers are undermining any sense of community in the workplace" (in Whitaker, 1999:105). Employees need to be able to maximize use of the technology being provided, and yet monitor themselves by being aware that their e-mail privacy can be invaded at any moment. Such a self-regulated, self-disciplined environment increases the level of social control within the workplace.

Employees who use e-mail lack any legal protection when it comes to issues of e-mail privacy. In Canadian and US courts, e-mail is not considered to be an electronic document protected under privacy laws (Lind, 1998:IT11). Employees therefore should not assume that absolute privacy can be achieved with respects to e-mail. Programs such as Mail Cop, monitor and even alert employees if "their e-mail is in violation of company policy," searching for key words or addresses that might alert the program that such an e-mail should not be sent or received (Lind, 1998:IT11). Thus, employees are given little leverage when it comes to e-mail, creating a need for legal precedents that would somehow protect both the employee and the employer.

Although some, such as Alan Gahtan, claim that the monitoring of e-mail in Canada by employers is in potential violation of the Criminal Code section 184, which prohibits "interception of private communication," the general consensus is that it is extremely difficult to assign concrete legal precedents to the monitoring and use of e-mail

(Fitz-James, 1999:E4). Employment and labour lawyer Howard Levitt points out that "there is no such thing as an absolute right to privacy in Canada," and yet at the same time, we cannot be asked to do such tests as lie detector tests in the workplace (Evans, 1998; Levitt Interview on CityTV, 1998). It is not a matter of *if* an employer can monitor an employee, but rather of the *limit* of the employer's conduct (Evans, 1998).

With regards to e-mail, Levitt's view is a popular one, namely that an employee's e-mail is not the employee's property but the company's (Evans, 1998). In the US, e-mail documents have been used in court cases many times. Aside from the most infamous case regarding Bill Gates (Lind, 1998:IT11), in which his e-mail was used in antitrust hearings, lawsuits against such companies as Epson America Incorporated, Nissan Motor Corporation and The Pillsbury Company, have focussed on the retrieval of e-mail documents, and the monitoring and interception of such documents. All three of the latter cases involved lawsuits claiming that the employer invaded the employee's right to privacy when monitoring the employee's e-mail. The Epson case was dismissed as the judge found that no state penal code was violated. Bourke vs Nissan Motor Corporation was similarly dismissed as the court "rejected the violation of privacy claim," and the Pillsbury case resulted in a similar decision (Pedeliski, 1997). In the Pillsbury case, even though Pillsbury stated that their e-mail messages were confidential, the judge ruled that the interception of e-mail messages was not an invasion of privacy because the "company is not...requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects" (Rosenberg, 1997:305). In addition, the judge claimed that "the company's interest in preventing inappropriate and

unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments" (Rosenberg, 1997:305). It was ruled that the prevention of communications that can be potentially harmful towards the company or the prevention of communications which are deemed unprofessional "outweighs any privacy interest the employee may have"(Lewis, 1997).

E-mail therefore, is rarely considered a private communication before the law. However, this does not mean that steps towards protecting the employer's and the employee's right to privacy should not be taken. E-mail privacy might be a difficult goal, but notifying employees about potential e-mail monitoring should always be considered. By informing an employee that one's e-mail can be monitored, the invasion of privacy is lessened because there is a level of consent that has been established. Employers have the right to know what their employees are doing, but at the same time, employees have the right to know if they are being monitored. Although some may argue that a good employee should have nothing to hide and thus privacy is not an issue, covert or secretive monitoring inherently invades an employee's privacy. It is not a matter of what information is being monitored, but the fact that private information *is* being monitored. Just because some believe there is nothing to hide within or outside the workplace, that does not justify the right to expose personal information. With regards to e-mail, privacy can become protected by either a written policy, which states that an employer will not invade an employee's e-mail privacy, or privacy can be established through a Foucauldian self-discipline process, where an employee knows that his or her e-mail is being monitored and thus accommodates such an intrusion by forgetting the candour of e-mail

and assuming that someone is reading it (Lind, 1998:IT11).

In terms of policies, tech-use policies - policies that deal with the use of workplace technology and the limits to which one's privacy is protected when using such technology - are becoming extremely popular in Canada and the US. A typical model policy should "reserve a company's right to review and intercept messages," as well as protect the "company's intellectual property in such things as documents and software" (Fitz-James, 1999:E4). The Ontario Information and Privacy Commissioner (1994) has set up some guidelines in the last decade that employers and employees should be aware of when dealing with the monitoring and use of e-mail. Some of the more important guidelines include informing the employee to what degree e-mail messages are confidential, encouraging employers to set up appropriate security measures to protect e-mail, and informing employees that e-mail can and will be monitored. By lifting the cloak of secrecy around the monitoring of e-mail, employees become more aware of how "private" their daily workplace communications are. Legally, employees have little privacy protection when it comes to e-mail, but the knowledge that privacy can be invaded can be useful in determining what information is to be sent via e-mail and when it should be sent.

Genetic Screening and Monitoring

Deciphering the genetic makeup of the human body and analysing the body's DNA codes in order to determine one's present, past, and future health sounds like science fiction, where cyborgs and clones populate the planet and databases of our genetic

identities crowd a warehouse or computer mainframe. But the modern exploration "into the genetic microcosms" is a real scientific and medical voyage in search of a "potential dangerous treasure," and medical wonders (Privacy Commissioner of Canada, 1998:1). Genetic screening and monitoring are present-day wonders which pose potential threats towards privacy, and at the same time reassure employers of the health of the individuals that are working for them. Genetic screening is a one-time process that can detect certain genetic traits linked to certain diseases while genetic monitoring "ascertains whether an individual's genetic material has changed over time due to workplace exposure to hazardous substances" (US Department of Labor,1998:3). The search towards unlocking the gene in the 90's, parallels the "unlocking of the atom in the 40s" (Privacy Commissioner of Canada, 1998:1). In both cases, "the excitement of discovery dulled critical assessment of the implications" (Privacy Commissioner of Canada, 1998:1).

On the one hand, there is excitement regarding the possibility of being able to predict health risks for certain individuals or being able to understand the possible side effects that certain job hazards might incur. On the other hand, there is a danger involving the ability to monitor and predict related and unrelated health concerns that are uncovered through genetic monitoring and screening. Legally, the use of genetic monitoring and screening in the workplace in Canada is hardly contested. This is mainly because genetic screening in the workplace has been rarely used thus far, with very few businesses admitting they indulge in such a method of potential surveillance in Canada[9].

---

[9] In 1990, the Canadian Manufacturers Association "knew of no genetic testing by its members," while a 1991 report of the Science council of Canada "found no workplace programs to screen potential employees for genetic susceptibility to disease" (Privacy

Genetic work also finds itself in a rather undefined area of law. Although discriminatory laws found in the Canadian Human Rights legislation do cover discrimination against those who are "perceived" as disabled, the collection of genetic information is legal as it is "unclear...whether individuals with genetic predisposition to diseases will be covered by the Code given that the perceived disability takes place in the future" (Ontario Law Reform Commission, 1996:136). The ability for genetic information to predict the possible biological future of an individual makes it hard for legislation to consider any sort of pre-employment genetic screening illegal. How can the law regulate the possible and not the probable future? Nonetheless, privacy advocates and the Ontario and Canadian Privacy Commissioners all make similar recommendations in restricting the collection and dissemination of genetic information.

The major concern regarding genetic information is how such findings impact upon employee surveillance and threaten privacy. Both genetic screening and monitoring have altered the world of surveillance by adding the element of prediction. Genetic surveillance surpasses traditional forms of surveillance as not only is one's past and present life being monitored, but one's future is also being monitored or mapped out.

Commissioner of Canada, 1992:16). Also, the Ontario Law Reform Commission reported in 1996 that they found little, if any, genetic testing taking place among Canadian employers (Ontario Law Reform Commission, 1996:159) The same cannot be said about the United States, where studies of Fortune 500 companies, utility companies, and unions showed that a small percentage of companies were involved with some sort of genetic screening or monitoring or a combination of both (Privacy Commissioner of Canada, 1992:17). However, the studies showed that there has been little or no growth in the companies doing such monitoring and screening between 1982 and 1990. Granted these finding are slightly dated, I have found little evidence of an increase in genetic testing by employers in Canada to date.

With genetic screening and monitoring in the workplace becoming a distinct possibility, employees become potential subjects of several years of surveillance in an instant. Genes can potentially show the medical history and future of its owner. An employer can conclude probabilities regarding an employee's or potential employee's future health and thus deal with that person accordingly. The ability to predict an individual's future and hold that individual accountable for their genetic makeup and possible health risks has privacy advocates and medical ethicists demanding legal protection. Genetic testing, although graced with the promise to be able to identify criminals through genetic fingerprints linked to deviance and aid in the improvements of workplace safety, also presents a "number of dangerous privacy exposures, since results of genetic testing reveal not actual diseases but only a probability that one might, at some time, contract a disease" (Smith, 1994:196). The collection, storage, and implications of genetic information threatens privacy from a physical, social, and legal standpoint. Genetic information can become costly from the perspective of individual privacy, while becoming cost effective for employers.

Once again, the line has been drawn between employer benefits, productivity and efficiency, *and* employee privacy. Employers can use genetic screening to weed out potential employees with potential health risks, by denying training opportunities, jobs or benefits to employees who possess particular genetic traits. Also, since "some genetic traits are found more frequently in specific racial or ethnic groups, such discrimination could disproportionately affect these groups" (US Department of Labor,1998:1). Denying an individual a job based on genetic information is an attempt to save the company

money, insurance deductibles, and potential future health costs. For the potential employee, however, it is a biological label, a genetic leash which has designated the individual as a possible financial burden to any employer. Information locked away in an individual's genes, unknown to the individual, can be costly only when such information is discovered. How potentially dangerous is genetic information? The Office of the Privacy Commissioner of Canada claimed that "no surveillance technology is more threatening to privacy than that designed to unlock the information contained in human genes" (Privacy Commissioner of Canada, 1992: 2). One must be careful when making such a bold statement, however, as genetic information on its own is not dangerous. It is the storage, the use, and the implications of such information that can be dangerous.

In a society which already fears that privacy has been lost, dead or relegated to a simple legal dilemma, genetic information adds a new complication to the already complex issue of surveillance and privacy. Genetic testing, monitoring and screening all challenge the notions of surveillance and privacy because a new form of accountability is brought to the forefront. Thus, a new element of surveillance, that of prediction, becomes increasingly important. Now the individual is even more accountable when it comes to genetic information. However, the individual has little control over such accountability and little choice in volunteering such information. The individual can volunteer a blood or hair sample, giving them a certain degree of control, although there is no degree of control over what information is collected through the genes obtained in this sample. Hence, an individual cannot change the genetic information he or she has or relinquishes for analysis. Accountability becomes minimized because the information provided

through such testing cannot be changed. Unlike the monitoring of e-mail, where individuals can discipline themselves not to waste company time with personal e-mail, the panoptic function of discipline disappears with genetic information. An individual can not regulate one's own genes.

The monitoring of video surveillance and e-mail can allow an employer to predict where someone will be or what someone will do based on repetitive patterns. But genetic information is not based on monitoring over time. It is a single episode of surveillance[10], that reveals information that can be relevant dozens of years down the road. As Nock points out, genetic surveillance projects self-contained reputations (Nock, 1993). Thus, privacy is even further threatened with genetic information because an employee loses the control or ability of self-discipline. The employee's future is already determined in terms of potential individual health risks and potential health costs that a company might have to deal with.

Video Surveillance

The third method of surveillance in the workplace I wish to discuss is that of video surveillance. Within the confines of the office, video cameras focus on the employees, and the customers if needed. The images the video camera collects are unbiased, for the camera merely collects the image that is within the path of its electronic eye. What is

---

[10] I am referring to genetic screening only. My concern is not with genetic monitoring and the potential hazards of the workplace (ie. chemical hazards).

done with the recorded information is another matter and of far greater concern. Video cameras, video surveillance, and CCTV are commonly referred to as tools against crime, or at least methods of crime prevention - a rationalization for the use of video surveillance within the workplace. However, that is only half of its purpose, as video surveillance is also used to evaluate job performance. Employers "frequently state that they simply see video surveillance as an effective means of improving security and in some instances specific functions such as improving quality control and maintaining compliance with regulations" (Privacy Committee of New South Wales, 1995:12). From an employer's standpoint, video surveillance is used for the good of the whole. It is intended to protect their employees as well as protect the business from potential financial losses due to such things as employee incompetence, internal theft, and inefficiency.

In contrast, from an employee's point of view, the use of video surveillance goes beyond mere benign protection. Accepting the fact that there are certain benefits for the employee, the main concerns regarding such monitoring revolve around the fear of excessive employer control, the invasion of privacy, the violation of basic human rights and a increasing level of mistrust directed towards employees from their employers (International Labour Organization in Privacy Committee of New South Wales, 1995:12). Roving eyes within the workplace add an element of insecurity amongst the workers, contradicting the security that employers' claim the cameras should ensure. This element of insecurity develops because employees may feel that they are being constantly monitored. What about lunch breaks and regular breaks? Do the cameras turn off when a worker is off the clock? Employees lose an element of privacy when always being

watched and may feel pressured to the point that their work might actually suffer rather than improve.

Video surveillance outside of the workplace, similar to the historically intrusive element of drug tests, is also a tool used by employers. The use of video surveillance outside of the workplace to gather evidence of "employees performing acts, while supposedly unable to work, inconsistent with their alleged disability," has become a tool for collecting evidence used in arbitrations (Luborksy and O'Reilly, 1997). From the employer's perspective, video evidence is not always admissible. As Gordon Luborsky and John O'Reilly (1997) discovered, the use of video evidence in arbitration cases in Canada dating between 1990 and 1996, did not always provide absolute evidence. Instead, in several cases, arbitrators had found that "where evidence has been secured at the expense of an employee's privacy rights, seeing is not always believing" (Luborsky and O'Reilly, 1997:1). Video evidence was rejected on several accounts because of an infringement of employee privacy; despite clear employee deception showcased on tape. Teleconferencing and video conferencing also raise some concerns regarding external work environment surveillance. Video conferencing is a useful tool in communicating to several people in different locations, but the potential for surveillance and privacy infringement is a serious concern. As Cynthia Ross-Pederson points out, video conferencing technology can be used when conferences are not in session, as "between video conferencing sessions there are large spans of time where the technology is readily available" (Ross-Pederson, 1997:9). However Pederson's concern in this case is not only privacy, but the difference between *spying* and monitoring. Another form of external

surveillance is the surveillance of workers who work at home but who are connected to the office through their computers. In this case, even though the employee is in their own home, the potential for their e-mail messages and computer work to be monitored is a possibility, especially if the worker is hooked up, online, to the company's main server.

The use of CCTV for surveillance in the workplace shares a few similar traits with the monitoring of e-mail and genetic screening. All three methods of surveillance involve the manipulation of time and space. E-mail monitoring can be done at any time, with e-mail being traced, recorded and retrieved from a central location completely separate from where the e-mail originated. As well, the history of an e-mail message is extremely difficult to destroy as is the message itself. In comparison, genetic screening searches for the genetic traits that disclose vital and extremely personal information. The monitoring of genes tags the subject with a biological leash, a genetic ID bracelet divulging past, present and possibly future information. Similar to e-mail surveillance, genetic analysis is done far away from the subject. Technically, the individual does not even have to volunteer for testing, as genetic traits are found in hair and skin samples.

Video surveillance also involves the manipulation of space and time. A CCTV system can be set up anywhere, with those that watch the video feedback geographically separated from those being watched. The video images can be recorded, rewound, fast forwarded, and monitored. Information can be played back over and over again. Once the image is captured, it can be broken down into pixels, manipulated and enhanced. Video camera technology adds a haunting element to surveillance because the camera captures the images, feeding off whomever enters its gaze. The camera is always there,

always recording if desired, creating its own space in the sense that entering a certain space puts one in the path of the electronic eye. The camera, in comparison to the shopkeeper, projects a "hypervigilant gaze," randomly scanning (Staples, 1997:4). Video surveillance can be extremely intense with around the clock zooming, telescopic and roving capabilities expanding its space. With such capabilities, it is no wonder employees fear for their privacy.

What video surveillance brings to the workplace, however, is not only a fear for privacy, but also an element of discipline. The surveillance is potentially constant, because unbeknownst to the employee the camera might not always be on them or even switched on. The impact of this surveillance is the illusion that a supervisor is constantly there. Although employees might feel violated because there is already an implied level of mistrust between the employer and the employee, employees might tend to watch their conduct within the workplace accordingly, so that their actions are not seen as suspicious or negative. Employees thereby become involved in a mechanism of power where they discipline themselves because they are aware that they are being watched, but unaware of exactly when. The panoptic function has once again reared its head. Employees can go out of their way to behave "normally" on camera and thus theoretically, order, efficiency, and control would result.

However, this panoptic function via video surveillance assumes that employees will go out of their way to appease the cameras, and more specifically the employers who watch the video. As mentioned before regarding the donkeys in the smart machine, employees might go out of their way to avoid being caught by the cameras by finding

unsupervised locations. Also, the element of self-discipline only works if the employees actually care about the video surveillance system; in many cases, video cameras merely become part of the office decor (Schuurman, 1995). Over time, employees might no longer become threatened by the cameras because the cameras are forgotten about and ignored. Furthermore, the cameras are only useful if consequences are felt when deviation occurs. If the cameras catch a deviant act within the workplace, and no immediate sanctions are taken against the employee in question, how does that reflect on the usefulness of the camera? But the camera, although docile on its perch, does not necessarily need to be accompanied with punitive sanctions. Instead, the threat of the camera, the threat of possible consequences establishes an element of fear and cautiousness. It is the threat of action that becomes the disciplining function of the camera, and the subordination and self-discipline of the employee, because of that threat, is attributed to the camera's presence.

Finally, a video surveillance system also possesses the element of prediction. Unlike genetic traits, no employee can be reprimanded for what one is *about* to do in front of the camera, but the video surveillance system is put in place based on the assumption that something *will* happen. (Staples, 1997:6). Similar to the monitoring of e-mail, video surveillance is preventing and predicting deviance "rather than responding to a violation after it has occurred" (Staples, 1997:6). Genetic traits lay out the potential biological future of an individual, while video surveillance is set up to catch a future deviant act. In the context of social control and surveillance, a degree of prediction is always present (Staples, 1997).

Avoiding or ignoring the eye of the camera however does not negate the problem that worker privacy is being violated. Ignorance of the camera's presence cannot be bliss. The social and legal implications of worker privacy violations due to video surveillance is what is at stake. Elements of trust and privacy become sacrificed within the confines of the workplace, perpetuated by the use of surveillance in an effort to enhance productivity in an era dominated by capitalism.

What are We Left With? - Elements of Social Control, Surveillance, and Privacy

Some of the groundwork for why surveillance is found in the workplace has already been done in chapter two. However, there is a need to further explore the phenomenon of workplace surveillance to grasp an even better understanding of the relationships found within the workplace involving the worker and the employer, the information being collected, the technology of power, social control, the concept of discipline, the concepts of trust and privacy, and finally, enlightening the worker through the development of employee self-awareness.

Social Control

After all the methods of monitoring have been laid out and specific instances of privacy invasion have been brought to the forefront, what exactly are we left with? What does this mean for the common employee? All of these methods of surveillance in the

workplace suggest that there is indeed an intensified, historically consistent form of social control; that in a postmodern society there is a blurring of lines between the public and the private; that identities are defined and redefined within the confines of the workplace; that privacy has slowly become a legal issue rather than a social/human rights issue; and that the workplace not only is indeed modelled to increase productivity, but also it is an environment bent on creating a "perfect worker". We are left with a transparent society (Brin, 1998), a controlled workplace, and a panoptic state that is "increasingly future-oriented and concerned about the predictive power of the information it gathers, just as the capitalist corporation is oriented toward the future return on its investment" (Whitaker, 1999:45).

Yet, the surveillance of workers is much more than prediction, as the workplace is responsible for creating, moulding, and defining its employees through surveillance. Privacy becomes constantly redefined, left behind, and infiltrated within the workplace, as employers establish more control and employees, consciously and unconsciously, relinquish their private lives. However, employees do not simply become pawns. There is an element of resistance against surveillance within the workplace, although for those where resistance fails or is only partially successful, surveillance becomes a method of social control implemented by the employer. Total resistance against surveillance becomes extremely difficult, mainly because surveillance provides the information needed to establish a disciplined workplace based on a privacy trade-off relationship. The workplace, the community that the workplace is found in, the city that the community is found in and so on, have all become part of a surveillance system. It is a system that no

longer necessarily functions from the top down, but rather surrounds us, becomes us, feeds off of us and supplies us with knowledge and power. As Staples points out, "disciplinary power, then, is thought of as being "bi-directional," not simply operating from the "top down" but circulating throughout the social body (Staples, 1997:25).

Therefore, perhaps what is needed is a re-evaluation of privacy. To confine privacy to a legal context is not doing the concept justice. Granted legal protection of privacy is warranted, and by all means when a severe violation of privacy occurs, then legal protection, of either the data or the employee, should be one of the answers. But it is much more than a legal problem; it is a social relation which has been questioned, challenged, reaffirmed and even disembodied. Privacy has been partially removed from the employee, placed in the hands of the employer, the government, one's co-workers and society. Privacy as a social relation, embodies efficiency, surveillance, and discipline within the confines of the work cubicle.

The workplace cannot be considered as an isolated environment but rather one that is influenced by the society of which it is a part. Elements of surveillance found within the workplace are part of a greater context of surveillance. Although there is no one Wizard[11] behind the curtain, monitoring and forcibly controlling us all in some Orwellian state, there is an element of a network, of a surveillance system that is as great and maybe even greater than the sum of its parts. For example, according to Abbe Mowshowitz, affinity groups, a collection of individuals with similar objectives, is able to shape the attitude of members - which is the essence of social control (Mowshowitz, 1996). Despite

---

[11] I am referring to the Wizard in the 1939 classic, *The Wizard of Oz.*

the great distance between these groups, all of whom are linked by one or several characteristics, with technology and communications improving at a phenomenal rate, these affinity groups can expand their roles (Mowshowitz, 1996:80). Mowshowitz uses the network marketplace to demonstrate this aspect of social control. For marketers and advertisers, computer networks facilitate a wide range and scope of target marketing which in turn will bring in more affinity groups into the network marketplace and thus expand the web of social control. Another key component with regards to social control and the network marketplace is that the consumer has become linked to the network via computers, phone lines, and televisions. Purchases can be made from one's home or office, but either way, the consumer becomes pulled into the network. Once integrated into the network, the consumer becomes a profile, a data file stored away for future reference. But the individual consumer is not alone, for what has happened is that all these consumers, no matter what their tastes are, have all entered affinity groups based on consumption and as Mowshowitz points out, "affinity groups based on consumption constitute the most likely arena for the elaboration of the new forms of social control" (Mowshowitz, 1996:97). Essentially, once one becomes involved in the network marketplace, one becomes linked to many other consumers, but also targeted as an individual consumer by marketers. Those consumers with similar profiles, get targeted as a particular affinity group. And it is this group, the virtual affinity group, that becomes moulded and defined, but will also eventually "develop its own norms and standards," as internal and external control mechanisms are implemented (Mowshowitz, 1996:98). Members of a certain affinity group begin to communicate with each other and the

opportunity for a virtual group formation via e-mail and file transfers establishes an element of endogenous social control. Thus, social control is imposed upon and internally generated by the members of the affinity group. It is this network that links us to others and to some degree implements a level of social control. Therefore, in some capacity, we all become part of the web of surveillance, part of the network or "system" of surveillance, and become incorporated into these affinity groups. This can happen in the workplace, or external to the workplace, but nonetheless, in some manner, we become part of a network which knowingly or unknowingly links us to others and at the same time incorporates us into a web of social control .

As mentioned, we feed off this element of surveillance, and thus, we ourselves become the creators and victims of increasing social control. Oscar Gandy points out that through surveillance, the ability to predict and prevent deviance makes the employee "the target of bureaucratic control," which is what is happening within today's work environment (Gandy, 1989:65). Based on Frank Webster and Kevin Robins' point that information technology is a complex social relation, Gandy concludes that the development and spread of information technology, which includes the surveillance methods used to gather information, "reflect the design and interests of bureaucracies and, increasingly, the consent and assistance of a "disciplinary state" that contains dissent and opposition from those least well served by the information revolution" (Gandy, 1989:65). Webster and Robins make the argument that the control of information technology and information itself is combined with "controlling the production process," and that the "history of capitalist industry...has been a matter of the deepening and extension of

information gathering and surveillance" (in Mainprize, 1996:11). Thus, social control is implemented through information technologies by processing and classifying workers and in addition, planning a certain behaviour within a social environment (Galbraith and Beniger in Gandy, 1989:65). Social control is implemented through the use of surveillance techniques within the workplace in an attempt to establish bureaucratic control, discipline, enhance productivity and create the docile worker.

Of course, it might be much simpler than that. Brin (1998) points out that it is human nature that drives us to want to know more about others. At our core, Brin argues, we are "information pack rats and inveterate correlators...we hunger for news, facts, and rumours" (Brin, 1998:80). Thus, we all crave information, and legislation of any kind limiting our means of gathering information will eventually fall on deaf ears. But do we crave information or do we crave what we can do with that information? It might be human nature to want to be nosy, but the gathering of information alone is not the problem when it comes to information technologies. Rather, the problem is how that information is used, collected, and disseminated.

What is of concern is the logistics of the "gaze", privacy within the workplace, and the dimension of prediction. The gaze of the video camera for instance is one that is intriguing and yet can violate an employee's right. It is intriguing because, as William Staples (1997) points out, we are a voyeuristic society and "we have become obsessed with the gaze of the videocam, not only because we perceive that it brings us "security" but also because we are fascinated by the visual representation of ourselves" (Staples, 1997:57). We are caught within a gaze that we might essentially *want* to be caught in.

But wanting to see ourselves and exhibiting ourselves does not mean we want others to know about us. Would it not be perfect if we could expose ourselves and yet reveal nothing? Unfortunately the gaze, the video captured, and the images recorded, do tell a story of normality versus deviance. Video surveillance tries to ensure normality within the workplace, at the expense of privacy.

The gaze itself however, is not perfect. First of all, is the gaze focussed? When a video camera surveys its allotted area, does it capture what it needs to capture? Video surveillance is usually automatic, independent of its owners and controllers, gathering video images without discretion. Within the workplace, if the video camera is a roving camera, then there is a chance that not all is being recorded. Then again, with several cameras in place, and overlapping "media" spaces being covered by different cameras, the gaze can be quite wide and consistent. With regards to the monitoring of e-mail, are all the e-mail letters being intercepted? Are only certain e-mail letters that contain key words being saved unbeknownst to the employee? The monitoring of e-mail is difficult to do consistently because of the manpower needed to weed through the mail. However, there are programs that can catch certain words that are deemed inappropriate and those letters can be looked at specifically.

Secondly, the gaze is no longer just a gaze. Video surveillance does not only videotape what is going on, but also can record and digitize a history of actions. Video surveillance goes beyond the gaze because there is a collection and analysis of information. Both e-mail monitoring and genetic screening have the same characteristics. Information gathered by these two methods of surveillance can be saved and recalled

easily, in an effort to create a file or database on certain employees. Finally, the gaze is bidirectional, where there is a need for both parties to voluntarily or involuntarily, knowingly or unknowingly cooperate in order for the relation to work. Although modern methods of surveillance are removed from their subjects and their controllers, eliminating face-to-face interaction, they are the tools of the omniscient observer (Zuboff, 1988:323). But these tools will only work if there is someone to monitor, someone to videotape, and someone to prick and probe for information. Without the subject, the gaze stares off in the distance, creating a "space" that would never be occupied. But there is always someone to watch, someone to monitor, and someone to spy on; we have *all* made sure of that.

Transformation and Disorganized Surveillance

Surveillance in the workplace is an actuality, but its purpose and effects are mysterious, confusing, and complex. Surveillance is mysterious because it can be hidden, yet exposing. Invisible and visible forms of surveillance within the workplace can be used to peek, prod and evaluate employees. Surveillance has been credited with the transformation of the workplace as well as the continuity of the workplace. Workplace monitoring has been argued to be either changing the workplace entirely or simply intensifying, modifying, and redefining it within historical scientific management strategies. Seen as either conducive or problematic to a more efficient work environment, surveillance in the workplace becomes a mediator of relations, a ruler for productivity, a

measure of compliance, and a safeguard for employers. Workplace monitoring tries to take away the uncertainties of the workplace, creating an environment where the employee becomes exposed.

But is the current workplace and the intensity of surveillance different now compared to early capitalist workplaces and if so, in what way? David Lyon (1994) argues that information technology and workplace surveillance do maintain the position of capital, intensifying employee monitoring. But viewing surveillance "in this light is to miss the broader significance" (Lyon, 1994:126). Lyon argues that new social relations are not produced through technologies, nor do they reproduce old ones, but rather computers control processes rather than people. An interesting point since others, such as Regan argue, that the workers are the focus and not the work itself (1996). Lyon explains that everyone within the work environment is prone to scrutiny and at times even the customer takes on the role of the manager, through customer response and needs. But this does not mean that the workplace is experiencing a total institutional transformation, where panoptic imagery, such as in Zuboff's case, implies total control. Lyon argues that the original intent of surveillance is misleading. Granted intensified surveillance can lead to greater control of employees, this was not the primary objective of surveillance. Instead, this form of control owes its existence to self-discipline and to enable "managers [to] derive extra control without bureaucratic or mechanical help" (Lyon, 1994:132). Thus, Lyon argues that the workplace and surveillance are not undergoing a transformation, but rather, as Dandeker and Rule also suggest, a form of continuity (Lyon, 1994:134). The enhancement of surveillance parallels the pursuit of "traditional goals of

co-ordination and information exchange between divisions and the internal supervision of the workplace, and in the quest for market niches, customer service and even 'electronic handcuffing'...of companies and clients" (Lyon, 1994:134). Thus, we are left with 'disorganized surveillance', a controlled workplace that is based on self-discipline and the compliance with norms. This is a type of workplace surveillance that is intense and revealing, but a consequence rather than an explicit means of coercive control through monitoring[12].

Lyon makes a valid point, claiming that technology and surveillance in the workplace must be seen "against the backdrop of changing patterns of economic enterprise and management," and as a significant departure from Fordism and not a novel social practice (Lyon, 1994:134). But surveillance in the workplace does more than only create control through self-discipline. Surveillance and technology within the workplace alter social relations through, what Poster (1995) calls, the "mode of information."

Before embarking on Mark Poster's poststructuralist concept of the mode of information, it is important to understand the power/knowledge relation. The place of power in the labour process involves a Foucauldian power/knowledge relationship (Sewell, 1996: Lyon, 1994). What becomes of utmost importance in the management of labour, is not only the accumulation of information, but the power/knowledge relation "which acts on the industrial worker under surveillance" (Sewell, 1996:790). Foucault argues that "power produces knowledge...[and] that power and knowledge directly imply

---

[12] See "Computerized Surveillance in the Workplace: Forms and Distributions," by James Rule and Peter Brantley (1992).

one-another" (in Sewell, 1996:790). Within the Panopticon, Sewell argues that "scrutiny and surveillance in the workplace are not arbitrary and indiscriminate, they are highly focussed and directed, reflecting the specificities of the power/knowledge circumstances" (Sewell, 1996:789). For Foucault, "knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised" (Foucault, 1979:204). Through the panoptic, one becomes visible, classified and sequestered, and discipline becomes an exercise of power. The visibility of employees assures the "hold of power that is exercised over them" (Foucault, 1979:187). But Poster focuses on another aspect of the power/knowledge relation. He argues that the categorization of people signifies their identity in society and that "language is not simply a tool for expression, it is also a structure that defines the limits of communication and shapes the subjects who speak" (in Lyon, 1994:191). Thus, the "electronic media alter(s) the rules of the game" (Lyon, 1994:191).

Poster questions the fixed subject in this "radical reconfiguration of language," where identity becomes unstable, multiplied, disseminated, and decentered (Poster, 1995:57-59). The mode of information, the reconfiguration of language, represents an unstable reality, a gap between the speaker and the listener, where the subject becomes lost. The subject is "interpellated through language and cannot easily escape recognition of that interpellation ...[thus] electronic communications systematically remove the fixed points, the grounds, the foundations that were essential to modern theory" (Poster, 1995:60). Therefore, the subject's identity becomes a shadow of its original self, a data image which is reconfigured as it flows from point to point, from

database to database. Social space becomes pervaded as the identity of an individual multiplies, without consent, intention, feeling or will (Poster, 1995:68). The physical subject becomes left behind, leaving a body with no soul. And it is within the mode of information that language becomes an act of domination, "a complex manipulation of symbols" (Poster, 1990:87). Ironically, we become producers of these identities, filling out forms for whatever identification card, thus we "actually participate in the process that multiplies our 'selves'" (Lyon, 1994:191). We are compelled, coerced, and persuaded to partake in the construction of databases, in the construction of our new 'identities', our new 'realities'. But what does this mean for privacy if privacy dissolves in power? (Lyon, 1994:191).

Lyon argues that privacy is socially constructed and if indeed we are created by electronic surveillance, then the power of this process to dominate us is far more interesting and pervasive than the socially-constructed private sphere being threatened (Lyon, 994:192). But personal interest aside, the multiplicity of our 'selves' begs the question that the problem of privacy has now been exacerbated. Labour relations and privacy relations between manager and employee no longer only exist at a legal level, nor do they only exist at a social level where privacy becomes constructed out of self-identity, but they now also exist at an electronic, database, and language level. Data images, the flow of information from database to database, and the reconstitution of an electronic identity become another privacy concern. A privacy concern that goes beyond self-identity because reality becomes reconfigured and identity, the original being, becomes misplaced, mysterious, and decentred.

Chip Off the Old Block of Privacy

After all is said and done, the main concern of privacy still remains a problem. There is a crack in the dam of privacy, one that leaks information that cannot be contained. Privacy, particularly privacy in the workplace, is continuously threatened and invaded in an environment infested with information technology and surveillance. An employee's privacy and identity are challenged within the workplace when an employer makes a conscious, and even unconscious effort at monitoring an employee and collecting personal information about them. Without repeating the various definitions of privacy already stated, it is important to explore exactly what is happening within the workplace in terms of violations of privacy. The problem with privacy is that it is a flexible concept, one that becomes defined by the situation rather than the individual. For an employee to establish a separation-based idea of privacy, it would relegate the employee into a realm of isolation. One could separate oneself from co-workers to an extent, in an attempt to maintain a level of privacy, but such isolation is hardly beneficial to the employee and such separation from one's employer is virtually impossible. With intense surveillance, hiding in one's cubicle becomes useless. Thus, an employee is relegated to a control-based idea of privacy, where the information surrendered is done with the permission of the employee.

Essentially, however, that is the problem. With increasingly persuasive methods of surveillance and a rationalization based on productivity, efficiency and control, the

voluntary aspect of a control-based privacy becomes threatened in the workplace. How can one hide information when they are being biologically invaded (genetic screening), constantly observed (video surveillance), and their work or daily activities are monitored (e-mail tracking)? There is however a voluntary aspect to surveillance and the relinquishing of information. Simon Davies points out that "many surveillance schemes now involve a 'voluntary' component which has the effect of neutralizing public concern about surveillance" (in Agre and Rotenberg, 1997:159). But is there really a voluntary component? Employees put their jobs at risk by not giving up information and not complying with business policies. As well, the voluntary aspect disappears when dealing with such methods of surveillance as simple video cameras in a work area *owned* by the employer. An employee is on the employer's property, and thus lacks significant leverage in controlling personal information. As Brin points out, can we even own our personal information (Brin, 1998)? In the debates mentioned earlier, many see control over personal information as control over property. But there are those who oppose such an approach. Roger Clarke sees the idea that information is a commodity as foolish because a more "useful convention is to recognize *interests* in data and in the case of personal data to recognize a very strong interest on the part of the data subject" (in Brin, 1998:91). Clarke states that claiming information as an inherent proprietary notion is doomed to fail (in Brin, 1998:91). In whatever manner privacy is understood, the problem that private information is being collected in the workplace is still of great concern.

But another problem regarding privacy, as David Nock argues, is that perhaps we have too much privacy to begin with. Nock considers the wide spread use of surveillance

techniques, which he narrows down to credentials and ordeals, as essentially the costs of privacy. With an increase in population and urbanization, there is an increase of strangers, which accordingly leads to an increase in privacy. Living in a world of strangers, it becomes difficult to establish trust with others without having some sort of "symbolic" measures of trust in place. These credentials and ordeals[13], credit cards, driver licenses, lie detector tests, and drug tests to name a few, act as signifiers of reputation. The information these ordeals and credentials contain establishes one's reputation, a reputation that can be transported anywhere at any time. Thus, one's reputation is portable, connected to its owner, and needed to establish trust amongst strangers. We have become strangers in a world that functions on trust.

However, Nock's thesis is difficult to apply to the surveillance found within the workplace. First of all, when a new employee is hired, it is a logical assumption that the employer would want to collect some background information on the prospective employee. The potential employee's previous credentials and past ordeals might be accessed by the future employer. Based on this information, assuming that the potential employee is qualified, the employer can achieve a certain level of trust between himself and the employee. But this social relation of trust, which was in need of being established when the employee was a stranger, falls to the wayside when the employer begins to monitor his or her employees. The element of trust that was originally established when

---

[13] The term 'ordeals' refers to rituals or rites of passage which aid in validating a reputation or determine if one is telling the truth. An example of an ordeal is a drug test or lie detector test. As Nock points out, through an "ordeal, people are able to validate their reputation, to garner proof of the validity of their claims, or to establish their claim to innocence, membership, or competence" (Nock, 1993:15).

hired disappears. One must redefine oneself within the workplace, establishing a new reputation through different ordeals and credentials. Secondly, Nock argues that we have too much privacy, but he fails to acknowledge the point that with ordeals and credentials, we become disconnected as well as connected to other strangers. We build relations of trust through surveillance, but we are left with creating relationships based on second or even third hand information. We become even more estranged from others and ourselves as our relations with co-workers and employers becomes reduced to ID cards, biometrics, and active badges.

But maybe we are really all coming closer together? Workplace monitoring is also an attempt at creating a workable workplace. As Mike Weir, a director at Computer Science Lab claims, the use of active badges, a type of surveillance, helps in the creation of a community. Weir argues that active badges "help people have a better sense of community through ubiquitous computing" (Weir, interviewed in Selling the Future, 1994). Thus, it is not just surveillance or the use of computers that is being sold, but the idea of community. Being able to tell where everyone is within the work environment brings us closer together. We are not spying on each other and management is not spying on its employees. Our co-workers are getting to know one another and management is getting closer to its employees, assuring them that they are there when needed. As Weir suggests, ubiquitous computing, which in this case can be classified as a form of surveillance as this includes active badges, "is for computers to get out of the way so people can do they want to do with their lives" (Weir, interviewed in Selling the Future, 1998). It is argued that a community built on surveillance and the knowledge of others

should be welcomed and not considered a hindrance but a facilitator towards trust and community. The workplace becomes a community because workplace control through surveillance is effective and consequently reflexive (Whitaker, 1999:40). Surveillance not only allows management to control the work, but the technology of surveillance surrounds us, enhancing the power of discipline and intensifying "the reflexive capacity of management to monitor its own performance and to take appropriate measures to improve its efficiency" (Whitaker, 1999:40). But workplace surveillance also becomes more than just enhanced Taylorism, the speeding up of production, but also a form of empowerment where there is a devolution of responsibility. As Reg Whitaker argues, surveillance allows for a delegation of power that progresses its way "downward from supervisory management to front-line or street-level worker" (Whitaker, 1999:115). Thus, it can be argued that surveillance in the workplace creates a community atmosphere, but one that is also based on greater dispersed responsibility. It becomes a matter of putting power back into the hands of the worker. The dispersal of information "simultaneously reorganizes the structure of supervision both vertically and horizontally...[and] computers in a sense allow individual workers to monitor themselves" (Whitaker, 1999:116). With this empowerment comes greater responsibility, but also greater vulnerability, as surveillance becomes decentred in the workplace and each worker becomes even more accountable.

The pace of collecting personal information within the workplace is increasing, but the value of this information is increasing as well. The information is being used in new ways with the goal being that it will have some strategic advantage (Smith, 1994:8-9). With new ways of using personal information, surveillance has become even more

intense in hopes of collecting every last bit of information possible; every piece of information is made relevant. But relinquishing information also allows us to participate in society and in the workplace. We are silently coerced and passively included into society through surveillance, through exposure. The legality of the right to privacy is a valid concern, but one that has its shortcomings. As an employee, there is a need to give up some information, since job evaluations depend on it. Management control, efficiency and social control require monitoring to some degree. But who is doing the monitoring, and what information is being collected and used become major concerns. The invasion of privacy, at least from a legal standpoint, grounds itself on the physical intrusion of space and the extraction of information, but depends on the self-protection of privacy[14] by those who can negotiate it (Lyon, 1994:196). Privacy based on social relations deal with self-identity, the construction of employee/employer relations, and the control of information. Within the workplace, the control of information becomes a crucial point. The control of information does not necessarily protect an employee's privacy, but rather gives the employee the ability to establish a position where only relevant information is exposed and collected. Control involves the construction of the self, either through impression management or data images.

My main concern is that employees should be aware of workplace monitoring and the social relations they are involved in which have allowed information to be collected. This point may seem trite, but it is only through the understanding of social, economic,

---

[14] The self-protection of privacy refers to placing the onus of privacy protection on the individual and, in this case, the employee.

and historical contexts that one can fully understand one's place within industrial labour in terms of privacy. Unfortunately, this does not clear up the privacy debate, but it does contribute to awareness of its complexities, for only out of awareness can we develop resistance. From a Foucauldian perspective, we must simply always be aware of the dangers. We must be aware of the potentials of privacy invasion - not only as a negative feature, as invasion has the undertone of negativity to begin with, but rather as a spring board towards an element of exclusion *and* inclusion in the workplace and society in general (Lyon, 1994:196-198). The increasing intensity of workplace surveillance is not a myth, nor is it the Orwellian Big Brother many make it out to be. However, this by no means negates employee concerns regarding workplace privacy. Despite the fact that privacy involves inclusion and exclusion, it does have limits. To what degree information is being collected, how it is being collected, and when it is being collected are still valid concerns. The problem is that privacy, as a participatory principle, lacks a true voluntary principle. Inclusion is only done because it has to be done, and this is no different in the workplace. Workers have to work to make 'ends meet' and they must act appropriately within the work environment to keep their job and maintain their quotas.

Surveillance in the workplace does create an aspect of employee self-discipline, but it also lends itself to the creation of the "perfect worker". It provides an element of control, power, and discipline as the employee is caught in the normalizing gaze. It is the creation of the "perfect worker" and the notion of prediction that allows us to look at surveillance in the workplace even further.

Creating the "Perfect Worker"

The final point I would like to make in this chapter is that employers are now not only trying to weed out those that are normal, the ones that work diligently, from the deviant employees, the ones that steal and waste company time; but also there is a conscious effort to create a "perfect" employee. In an attempt to predict employee actions in the workplace through surveillance, employers have consequently eliminated the employee characteristics that they do not want and have attempted to create an employee that fits the company mould. As Regan points out, "the trend is that surveillance increasingly focuses on the worker rather than the work itself" (Regan, 1993: 1). The work is secondary when it comes to monitoring, as the body is now the focus of surveillance. Staples furthers this argument, claiming that "the ability of organizations to monitor, judge, or even regulate our actions and behaviours *through our bodies* is significantly enhanced" (Staples, 1997:5). The focus is now on the worker and how that worker should act within the confines of the workplace. John Gilliom argues that an employer wants to maximize the labour of an employee, referring back to Richard Edwards' explanation of the aspect of control within the workplace and how the workplace becomes a battleground (Gilliom, 1994). Edwards claims that the "workplace becomes a battleground, as employers attempt to extract the maximum effort from workers and workers necessarily resist their bosses' impositions" (Edwards in Gilliom, 1994:48). By predicting and assuming the actions of an employee with the aid of surveillance, employers are aiming at creating a "perfect" workplace full of "perfect

workers". Gilliom claims that the drive towards production has become secondary to the drive for the "perfect worker" (Gilliom, 1994:50). The goal is to find the right person by eliminating the wrong person, not by necessarily working with what is given to you. Employers have the ability to hire and let go those workers whom they feel are needed for the company. Thus, "the premise that management concerns are limited to actual rates of productivity is outmoded. The contemporary approach to increasing discipline and productivity is a far more encompassing strategy that seeks to find...the good worker" (Gilliom, 1994:51). With the incentive to find the "perfect worker," personal information increases in value exponentially. With a laid out plan of what type of workers are wanted and needed in the company, the office becomes a mechanism of power with disciplinary power diffusing and circulating within, shaping and creating the perfect environment (Gilliom, 1994:53). And in the end, the employee becomes even more visible than ever before, forced to forfeit an enormous amount of personal information to the shopkeeper.

Chapter 4 - Privacy Satisfaction, Legal Action, Union Reaction

Do We Really Care?

A Life Less Ordinary and Private

What remains to be seen is not how surveillance in the workplace has come about, but rather, do we as individuals and employees even care that there is an element of privacy invasion, and how do we as individuals and through collective organization, ie. unions and governments, deal with the issues of privacy especially in the workplace? Also, are we dealing with the issue of privacy appropriately, as a social and legal issue? The concern is now redirected towards the individuals, the "victims" of privacy invasion, who are concerned that there is the ongoing possibility of personal information being accumulated, overtly or covertly; distributed; and manipulated.

We have become subjects in a society bent on exposing its citizens. We gain citizenship and other rights through the information we generate and at the same time are revealed by that same information, which is accumulated and distributed to other parties. As explained earlier, we have created our own world of privacy invasion and privacy protection because we continuously become a part of it, feeding it and living off it. The most pessimistic expert might even say that the "game is already over, that technology has laid bare the life stories of us all, that Canadians should consign the concept of individual control to history, stop worrying and learn to live with and love the free flow of

information" (International Labour Office, 1993a:30). However, the increase in cases of privacy invasion do not necessarily constitute a need for the complete elimination of electronic surveillance and in particular, job performance monitoring. One commission in France agreed with such a point, stating that "data processing should be controlled, not paralyzed" (International Labour Office, 1993a:30). Thus, I would argue that despite the fact that there is a fear of privacy invasion within the workplace because of workplace surveillance, this does not constitute the need for its outright elimination. I agree that there is an element of privacy invasion because of the surveillance of employees, but I also agree that employers need to have a certain level of information about their employees and employee performance.

Returning to Reg Whitaker's argument, he points to our "growing apathy about personal security breaches from our indoctrination into the panopticon society" (Martin on Whitaker, 1999). Through the elimination of risk, the panoptic features of our society elevate the intensity and range of surveillance, creating a large "network" of which we are all a part. We thus establish a dialectical relationship with this "network." Information technologies form two sides of the same coin as they "enable and empower, but they make their users more vulnerable to surveillance and manipulation...the two sides cannot be separated: it is precisely what empowers that also extends vulnerability" (Whitaker, 1999:101). For example, many people willfully volunteer personal information in order to receive goods or services in return. Privacy and information become involved in a reciprocal relationship where a loss of privacy begets a reward.

Frank Webster also makes a similar point regarding the relationship between

privacy and surveillance. Webster points out that one of the main paradoxes of modernity has to do with distinguishing between individuation and individuality. Individuation is when a person is identified by a singular record, while individuality, which many believe is being increasingly threatened, is the ability to be in charge of one's own destiny, "having genuine choices in and control over one's life - things immicable it would appear, to intrusive institutions and their information-gathering impulses" (Webster, 1995:55). Webster explains that the paradox revolves around the notion that individuation requires that people be monitored but "the development of files on individuals...may in fact be requisites of enhancing their individuality...(and) if we as a society are going to respect and support the individuality of members, then a requisite may be that we know a great deal about them" (Webster, 1995:55). Thus, a paradox emerges: there is a tendency for the need of greater surveillance in order to safeguard individuality.

On the one hand, the need to surrender information can be seen in a positive light, as more information about people establishes a greater degree of trust and equality between members of a society. Webster goes on to explain that personal information is needed so that individuals can receive certain entitlements and a certain level of individuality (1995:56). Hence, "we cannot...straightforwardly equate greater information about people with a diminishment of individuality," and thus, another paradox emerges stemming from the idea that the world is now a world of strangers (Webster, 1995:56). We live in advanced, complex societies which need to gather detailed information about "their publics in order to function" (Webster, 1995:57).

On the other hand, the act of "volunteering" information is not as voluntary as one

would like to think, especially when information is needed to become part of an information driven social system, found inside and outside of the workplace. One must be able to give up information for something in return. Therefore, it is no surprise that the invasion of privacy is significant, yet the invasion's impact is lessened by the need to participate in society, and the general apathy about relinquishing information. It is no different within the workplace. Although surveillance and the gathering of information are an integral feature of all modern societies, ignorance is not bliss, and apathy or the lack of concern over surrendering information is not a suitable or justifiable explanation for the invasion of privacy. As far as the workplace is concerned, it is still not entirely clear whether there is a "need" for employees to waiver information in order for them to become part of the business organization. As corporations get larger, become bigger players in the community, and provide more goods and services, the surveillance of the shop floor becomes even more crucial in attempts to maximize efficiency. However, is the invasion of employee privacy necessary? Also, it is necessary to evaluate if the employee or the citizen realizes the consequences of surveillance in terms of what information is being collected and how their privacy is being invaded. How can an employee complain if he or she does not realize what is happening or even care?

Privacy in Canada Revealed

At any given moment in the workplace, a piece of information about an employee can be retrieved and recorded either overtly or covertly. In addition, the ability to avoid

such means of surveillance and still be able to fully participate within the workplace, i.e in employment, work benefits, and security clearance, is virtually impossible. In our search for security and convenience, are we hitching ourselves to an electronic leash, or are we simply experiencing the logical consequences of modernity, trying to establish some form of individuality as the lone individual caught in a growing world of strangers?

Secondly, it is important to understand the degree to which Canadians feel their privacy is violated. One of the biggest and most recent studies done in Canada (Ekos Research Associates, 1993) reveals that privacy has become a growing concern among Canadians, although workplace privacy is only of minor concern. The study, based on 3000 respondents, found that 92% are at least moderately concerned about privacy while 52% of those Canadians who experience some concern are extremely concerned about privacy. However, a ranking of different types of privacy showed that workplace privacy was ranked the lowest; mainly, the analysts argue, because monitoring at work is generally explicit. In terms of balancing privacy, or achieving an acceptable level of privacy in return for entitlements, the study showed that "meeting the condition of informed consent," made the provision of information far more acceptable (Ekos Research Associates, 1993:11). Eighty-one percent felt strongly that they should be notified in advance when information is being collected, and overall, "many privacy intrusions are relatively more acceptable when there is a practical rationale or benefit" (Ekos Research Associates, 1993:12). The study also found that only 3% of those who experienced serious invasions of privacy experienced them in the workplace.

No matter how complex the study is, the researchers realized that overall, it is hard

to grasp the big picture in terms of how Canadians feel about privacy, and thus there was a need to further refine the research. As a result, they created a typology in order to deal with contradictory beliefs and perceptions of privacy among Canadians of diverse demographics. The typology allowed the surveyors to establish certain distinct types, five in total, that better illustrate the sentiments of Canadians regarding privacy. The largest cluster (31%) were found in those with the most anxiety and discontent about privacy and who feared that the government, as a regulatory body, had too much access to information. This group, composed of well educated individuals, had "deep seated concerns about surveillance, control and manipulation" (Ekos Research Associates, 1993:36). More than 50% agreed that there is no real privacy because either businesses or the government know everything and anything they want to know. These "regulators" also do not see adequate controls in place to deal with privacy issues and are thus "fearful of the threats implied by the interaction of technological change and the thirst for information" (Ekos Research Associates, 1993:35). However, the regulators do feel that the re-establishment of personal comfort with privacy issues must be addressed through informed consent and regulation (Ekos Research Associates, 1993:36).

The second largest group, the "extroverted technophobes," which represented 23% of the respondents, had similar concerns as those "fearful regulators." However, their fears were based on "the absence of any clear understanding of just what the nature of the threats are" (Ekos Research Associates, 1993:36). This group, made up of respondents who are likely to be poorly educated, economically marginal and found within the powerless sectors of society, are fearful of the unknown and yet ironically, "also claim to

be open and confident and more likely to dismiss privacy as a serious concern" (Ekos Research Associates, 1993:36). Both the regulators and the extroverts see the solutions to privacy problems in the hands of the government rather than themselves. This final point is what makes them different from the third type, the "guarded individualists" (6%), who are young individuals, tight lipped about revealing personal information and less threatened by new technology. They are cautious yet "confident in their individual capacity to deal with privacy threats" (Ekos Research Associates, 1993:37).

The "open pragmatists," who represent 22% of Canadians, represent average, middle of the road individuals. These respondents were classified as having "rather *average values on most attitudes*" (Ekos Research Associates, 1993:38). There is little concern among them about threats from new technology. However, they do "insist on the *need for informed consent,* and believe that some form of *rules are necessary* to protect the privacy interests of citizens" (Ekos Research Associates, 1993:38). Finally, the "indifferent" (18%), "acknowledge the reality of privacy threats" but do not "acknowledge its personal relevance" (Ekos Research Associates, 1993:38). They have an open and confident attitude to the provision of information.

Overall, the study found that privacy is a crucial issue in today's society, one that has drastically grown in importance over the last ten years. The study points out that "within Canadian society, there is a pervasive sense that personal privacy is under siege from a range of technological, commercial and social threats" (Ekos Research Associates, 1993:40). The study points out that most privacy concerns are not related to personal experience, but are rather based on other factors such as matters of principle and reported

experiences (Ekos Research Associates, 1993:41). In addition, privacy concerns were seen as a greater problem when individuals lacked awareness and control of the situation. High levels of concern were also linked to more abstract, unfamiliar threats to privacy, such as the linking of databases and covert monitoring. In the end, the respondents claimed that some forms of privacy invasion are merely nuisances, such as tele-marketing, where consent is given; while serious threats to privacy, which include covert monitoring, spying, the linking of data, the multiple uses of information and the sharing of information, created a level of fear which was uncomfortable and unwanted (Ekos Research Associates, 1993:42). A lack of control over one's information and over different forms of privacy intrusion was the biggest threat, as "the uncontrolled and surreptitious forms of privacy intrusions...are by far the most threatening and unacceptable" (Ekos Research Associates, 1993:44). Thus, serious threats of invasion were of the greatest concern to most Canadians and many seek "greater control, consent and protection" (Ekos Research Associates, 1993:44).

Protect Yourself - Hide Behind Your Desk or Put Your Faith in the Balance of Justice

Invasion and Protection - The Causes and Consequences of Privacy Legislation

What is also troubling about the invasion of privacy within the workplace is that the legal avenues for employee protection, as well as the means to defend one's privacy and information, are muddled. Recourse for employees regarding workplace monitoring

and privacy invasion is a complex process, more likely to find obstacles than a quick solution. Torts, non-existent privacy rights, human rights, and criminal codes combine to create a hodgepodge system of privacy legislation that misses the mark. Employees are left to deal with the consequences of privacy invasion, rather than finding suitable legislation that protects them from such an infringement in the first place.

In addition to privacy legislation being confusing and directionless, some have pointed out that the regulation of information technology and the protection of privacy is misguided, because the solution to the problem of privacy is part of a "complex knot of different tensions, rights and responsibilities," and the concept of privacy itself is lost amidst an array of definitions (Bennett, 1991:56; Chaffey, 1993; Davies, 1997; Regan, 1993). The policy making processes, the protection of data and privacy, and the various legalities involved are part of a larger problem - the inability to define and understand privacy.

Not only has the definition of privacy remained a thorn in the side of privacy legislation, a legislation that is ironically meant to clarify the issue, but there is also a conflict between ideas, interests, and rights when it comes to policy making and the creation of legislation (Regan, 1993). We have become so involved in an issue that is hard to describe and even grasp, so involved in finding a solution, that we have lost sight of the problem that instigated caution and such efforts in the first place. Also, we have become so consumed by the issue of privacy, that we do not know where to turn. We question the government, the corporations, and our employers, and in the midst of the confusion, we sometimes tend to leave ourselves out of the process. Unknowingly we

become pawns of the government, of corporations, and employers, even though we are the ones involved in this complex issue. Because they are uninformed, individuals have a tendency to refuse to take responsibility for their own privacy. Maybe refuse is a strong word, but we are reluctant to control what we are actually able to control, thus shirking responsibility. As Flaherty points out, there is a need to be more privacy-conscious (Flaherty, 1997:172).

Aside from being aware of one's own privacy, some might profess that we have already lost our privacy, that "nothing will protect or save privacy. It's over" (Brin, 1993). They might argue that the battle being currently fought is one against a traffic jam of information, a transparent society, a self-exposed community, and that the best way to think about privacy "is to behave as though you don't have any" (Manes, 2). That being said however, it should not discourage attempts to regain privacy if not to protect what has not yet been lost of privacy. Thus, despite skepticism, regulations to deal with privacy issues, information technology, and data protection rage on, and on a global scale.

Globally many countries including Sweden, Germany, the United States, Britain, and Canada, have made some strides towards dealing with information technology. However, dealing with information technology is a broad term and does not entirely or specifically include the issue of privacy, especially workplace privacy. Rather, there is an attempt not to protect the worker's or individual's privacy per se, but to protect a worker's or individual's personal information. The trend towards data protection has now a main focus of privacy, according to Bennett, as the problems of the future "will centre not so much around the technology, the individual, or the bureaucracy, but around information"

(Bennett, 1991:66).

Bennett contends that when dealing with the notion of privacy, three distinct definitions of the problem can be identified, and thus three different solutions arise (1991). First, there is the technological approach, where if one regulates the computer, this will consequently protect the individual. By this Bennett is referring to technological safeguards, where the input, storage, and retrieval of information is done only by those with the proper authority. A technologically determinist policy or legislation based on such an approach "makes no judgement about the propriety or necessity of information collection in the first place" (Bennett, 1991:57). Secondly, the problem is that privacy is seen as an individual civil right, where the concern is to protect individuality and integrity. As Westin points out, in order to have control over one's one information, "they must be given certain concomitant procedural rights" (in Bennett, 1991:59). However, Bennett also brings up the point, quoting Spiros Simitis (1987), that the more privacy and seclusion awarded to an individual, "the more the right to be let alone develops into an impediment to the transparency necessary for a democratic decision-making process" (in Bennett, 1991:60).

Finally, the third approach towards privacy is based on bureaucratic accountability, where technology is used as a tool for power. In this case, the issue of privacy is "not justified as an end in itself but as a means to control the power of the state" (Bennett, 1991:60). In conclusion, Bennett states that these three approaches fail to address the issue of privacy on more than one level, ignoring the "dynamic relationship between information technology and organizational information practices" (Bennett,

1991:63). Privacy is a complex issue which is not properly dealt with by earlier, and even current legislation.

By addressing all the social factors involved with privacy, information and the protection of information become the prime targets, as data protection would account for information privacy. However, data protection does not cope with the intrusion on privacy, but rather only the control over information. Although data protection is a crucial and valid effort, for the employee being monitored it provides limited help. The intrusive collection of information *itself* is a problem for the employee as well as the protection of the information that is accumulated through workplace monitoring. For the employee, the information being collected needs to be protected and used only for previously stated, work related purposes. It is a matter of dealing with the problem of privacy invasion as well as the consequences of data collection. The need for data protection within the workplace hinges on the fact that the invasion of privacy is a possibility to begin with.

Privacy Law and Order in Canada

Canada has made great strides in the field of privacy and information protection over the last twenty to thirty years, although mostly limited to the public sector. The establishment of a federal, and in some cases a provincial, Privacy Commissioner has allowed for a middle man to enter the privacy and information discussions. More than an Ombudsman, Commissioners have limited powers but are able to bring privacy and

information concerns to the forefront and the courts. Canada's ability to formulate laws and enforce mechanisms "both for greater openness and accountability for general information in society and for the protection of the personal information of the citizenry," makes the country quite unique (Flaherty, 1997:168).

Despite these accomplishments however, current legislation is stymied by the inability to define privacy and the inability to deal with the moral, legal and social implications of it. Rapid changes in technology have also hampered legislation. Ian Lawson points out that "the new reality of information...is that when [information] is combined with the latest in computer and telecommunications technology, it is beyond the ability of current legislation to address adequately" (Lawson, 1997:42). As well, Lawson explains that current information laws are mostly restricted to the public sector, not the private sector (Lawson, 1997:42).[15] In general, there are several torts, criminal laws, rights, and federal, and provincial statutes in place that are meant to address the privacy concerns of workers and individuals. However, federal and provincial statutes conflict, and there are significant differences between provincial legislation, causing legal instability.

---

[15] There have been strides made towards the protection of information in the private sector in the last year, especially dealing with E-commerce and offline business transactions as well. However Lawson does point out that "not only do few of our existing information laws apply to the private sector, but any existing laws that do apply are likely to be unable to cope with new information technology" (Lawson, 1997:42).

Provincial Statutes

Several provinces, including British Columbia, Alberta, Saskatchewan, Newfoundland, and Nova Scotia, have passed different versions of Privacy Acts over the last thirty years. With British Columbia leading the way in 1968, the Privacy Act mainly protects information in the public sector only, through the introduction of specific torts meant to deal with violations of privacy. Although the provinces' Acts vary to some degree in terms of the different torts that make up the statute, they are mostly hybrids of the British Columbia Act. British Columbia also passed a Freedom of Information and Protection of Privacy Act in 1992. The Act "prohibits the collection of any personal information unless expressly authorized by statute, the information is collected for the purpose of law enforcement, or the information relates directly to and is necessary for an operating program or activity of the public body" (s26) (Lawson, 1997:79). Thus, any information collected must be done with the understanding that the individual is aware of the purpose of the information being collected. Of course, this Act is only limited to public and governmental bodies.

In contrast, Ontario and Quebec seem to be going in opposite directions. Ontario lacks significant "legislation setting out general remedies for privacy invasion," while Quebec has taken the privacy concerns and data protection to the forefront, surpassing other provinces with legislation applying to both the public and private sectors (Lawson, 1997:96). Although Ontario did enact a Freedom of Information and Protection of Privacy Act, it adopts many of the provisions of the federal Acts, applying only to the

public sector. The Act did establish a Privacy Commissioner, the first of its kind, and the Act does require that information be collected for official purposes only, but there is no limit to the information collected nor does the Act "address the impact of computerization of personal information" (Lawson, 1997:96).

Quebec, on the other hand, offers protection to its citizens with its Civil Code, the Quebec Charter of Human Rights and Freedoms, Quebec's Act Respecting Access to Documents Held by Public Bodies and Protection of Personal Information, and most importantly, Bill 68, which is An Act Respecting the Protection of Personal Information in the Private Sector. Bill 68 is the key Act out of the four, as it applies to the private sector, unchartered waters for the rest of Canada. The Bill restricts the collection of information in the private sector, based on the legitimacy and the purpose of the information. It also protects individuals, by assuring that the destination of one's information is known and an individual can opt-out of any information collection acts. The Quebec Charter is also unique compared to other provincial Charters as it has specific clauses meant to protect one's privacy.

The Federal Act

As for federal acts, the 1982 Privacy Act and the Access to Information Act both apply to only the federal government. These acts were both inspired by revisions made to the Canadian Human Rights Act in 1977. The Privacy Act defines personal information and outlines regulations regarding the collection of personal information within the

federal government - although it is limited to certain federal agencies. Prohibiting the collection of unrelated personal information, assuring the direct collection of information from the original subject, and assuring that information is used for the single purpose for which it was collected, are some of the main aspects of the Act. A Privacy Commissioner, with broad powers and the ability to investigate privacy complaints and implement privacy legislation, was also established.

The Canadian Charter of Rights and Freedoms also attempts to provide some protection for individuals against the invasion of privacy. The Charter, in section 8, states that "everyone has the right to be secure against unreasonable search or seizure". This chartered right can potentially include the right to privacy. Although the Charter is restricted to the actions of government, and "arbitrators have generally declined to apply the Charter directly, many have taken "charter values" into account when defining the scope of employee privacy rights" (Luborsky and O'Reilly, 1997:3). Surreptitious surveillance of an individual has been challenged by section 8 of the Charter as it constitutes "an unreasonable search and seizure" (Luborsky and O'Reilly, 1997:3). However, the Charter also falls short of full protection for an individual and an employee, and is only one part of a complex, mismatched legal system meant to protect one's privacy.

Finally, most of the privacy legislation, both provincial and federal, is based on "fair information practices." These practices are "guidelines for the collection, use, disclosure, retention and disposal of personal information" (Task Force on Electronic Commerce, 1998:8). These fair information practices include issues such as public

awareness towards privacy issues, consensual collection of information, access to information, maintaining the accuracy of information and establishing the relevance of information. Nonetheless, federal legislation and acts are still a "patchwork" of laws, regulations, and codes and, similar to the provincial statutes, they fall short of protecting those in the private sector. As the Task Force on Electronic Commerce suggests, "while the patchwork is useful as far as it goes, it is not adequate in the face of new developments" (Task Force on Electronic Commerce, 1998:6).

The shortcomings of Canada's legal system and its inability to appropriately deal with privacy issues has not gone unnoticed. The current Privacy Commissioner of Canada, Bruce Phillips, acknowledges that there is a need to address privacy issues and a need to reevaluate the legal system. Phillips points out that there is a "pressing need to modernize the existing Privacy Act" mainly because "it is not truly a privacy law but a data protection statute"(Phillips, 1998:10). Phillips goes on to warn the government and Canadians, that "in fact privacy has surprisingly little protection in Canadian law; torts in some provinces and - as a last resort - the Charter" (Phillips, 1998:10). Torts, acts, and legislation that have gone untouched for the past 15 years need to be re-evaluated and modified to deal with advances in technology, data protection *and* the invasion of privacy.

The Right to Privacy

Although the above is only a brief summary of the provincial and federal acts and legislation, it is important to demonstrate how employee privacy and the monitoring of

employees inside, and at times outside, of the workplace is dealt with by both provincial and federal legislation, the Criminal Code and other codes. Perhaps what is most problematic when it comes to the Canadian legal framework dealing with privacy, is the issue of a right to privacy. The right to privacy itself is not guaranteed in the Canadian Charter of Human Rights and Freedoms, however it has been "recognized as a fundamental value in a number of Canadian Supreme Court decisions" (International Labour Office, 1993a:123). Under Section 7, an individual has a right to life, liberty, and security, a claim that is found in some provincial privacy acts and human rights legislation. More specifically however, any right to privacy or the protection of rights and liberties is actually derived from common law (Chaffey, 1993:117). Douglas Chaffey points out that similar to the United States, Canada's "common law and later statutory and constitutional development...(have) reflected the principle that a man's home is his castle" (Chaffey, 1993:118).

The use of common law to protect one's privacy raises two important questions. Is common law capable of protecting privacy, and is there an actual right to privacy in common law? The common law's ability to protect privacy has been criticized for being too flexible because court decisions on privacy create "idiosyncrasies and uncertainties in the law," and it would be wiser to put one's faith in legislation instead (Glasbeek in Lawson, 1997:148). A 1972 report supported similar frustrations with the common law, concluding that the "courts alone can provide only partial solutions to complex issues and social needs" (Lawson, 1997:148). Thus, the social needs of privacy cannot be adequately met through torts found within common law. Some supporters argue however, that it is

this flexibility that makes common law protection of privacy so appealing. Nonetheless, feasible or not, the right to privacy still lays in the balance of common law.

As a right, privacy would be equivalent to the right to free speech or a fair trial. However, Canada does not have a Bill of Rights, nor does the Charter of Rights and Freedoms distinctly outline privacy rights per se. As Lawson points out, the exclusion of such rights does not "mean these rights do not exist or are unenforceable," and that the right to privacy can be found within common law (Lawson, 1997:150). Common law allows for a "considerable degree of protection...afforded to privacy...as an incident to the law's protection of individual rights in other areas" (Lawson, 1997:150). The existence of other rights, affirms to some degree the right of privacy under common law and associates this right to other, already established rights. Although there is no free standing tort of privacy invasion, the courts of Canada have made steps towards recognizing the right to privacy, even though the right of privacy *per se* is non-existent in law (Lawson, 1997:155).

Workplace Privacy and the Law

Workplace privacy is not protected by any specific constitutional or statutory provisions, rather Charter principles have been applied instead (International Labour Office, 1993a:123). The issue of privacy is dealt with through search and seizure legalities found in the Charter as well as provincial human rights legislation. Electronic monitoring has been "characterized as a fishing expedition, where its use is not triggered

by specific evidence, but may be used to generate evidence of wrong doing" (International Labour Office, 1993a:123). Thus, the Charter must deal with electronic monitoring as an unlawful search and seizure procedure. As for the monitoring and surveillance of workers, there are no concrete provisions to regulate such practices found in Canadian labour codes. Therefore, the boundaries of surveillance are dealt with by the employee and employer via collective agreements (International Labour Office, 1993a:124). However, there are laws that do regulate certain aspects of surveillance, mainly the Privacy Act, the federal Labour Code and the Criminal Code, which deal with data protection, the intent of the information collected, and the interception of communications.

Electronic mail, for example, has perhaps become one of the biggest concerns in the workplace in terms of the monitoring of such communications. Under the Criminal Code, the interception of telephone communications without consent is illegal. The interception of e-mail, which is essentially a phone or cable communication, can be somewhat protected under Section 184(1) of the Criminal Code. However, if an employer warns their employees that e-mail can potentially be monitored, the Criminal Code will not apply. Some employers "explicitly state in their e-mail policies that e-mail is the property of the company and that employees should have no expectation of privacy" (Harowitz, 1998:49). This clause reduces the risk of violating the employees' legal rights (Harowitz, 1998:49). At the federal level, the Criminal Code does prohibit the interception of private communications, although the code allows for certain exceptions. To be "effective as an exception, any consent given under this section must be made

voluntarily and with complete knowledge of the consequences" (Lawson, 1997:116). These exceptions, which come under the pretense of general consent, are still quite ambiguous, as the Code provides exceptions which would allow "certain monitoring of employee telephone calls where there is no reasonable expectation of privacy...or the use of soundless videotape to monitor employees" (International Labour Office, 1993a: 124). What exactly is considered as a "reasonable" expectation of privacy remains a mystery under the Criminal Code. Maureen Fraser points out that the application of the Criminal Code in the employment context has been limited - no doubt because of its ambiguity (in Baarda, 1994b:15). Overall, the Criminal Code does not provide adequate protection against the interception of employee e-mail by employers, especially in the private sector.

Video surveillance, on the other hand, is neither prohibited nor explicitly permitted by the Criminal Code. However, legislation dealing with video surveillance is found under the Charter, once again under Section 8, the search and seizure clause. The issue of video surveillance is usually addressed in terms of the content of the video and the ability of the video to be used as evidence in a criminal proceeding or in "a disciplinary action against an employee" (International Labour Office, 1993a:132). Some have argued that without the consent of an employee, the video evidence gathered by CCTV can constitute unlawful search and seizure. In cases when the evidence is admitted, and the case goes to an arbitrator, the arbitrator will almost always "begin their analysis with a consideration of the award in *RE Doman Forest Products Ltd. and I.W.A., Local 1-357*" (Luborsky and O'Reilly, 1997:4). The Doman Forest case was a breakthrough case and an excellent example of the "liberal application" of the Charter (International Labour

Office, 1993a:133).[16] Section 7 of the Charter, which looks at the right to security in terms of the consent and knowledge that a form of surveillance has been practiced, is also applied to issues of video surveillance and the invasion of privacy.

Finally, genetic monitoring and screening might be the most difficult type of privacy invasion to protect in Canada and even the United States. This is mainly because it is a type of surveillance that is in its early technological stages. However, the potential privacy invasion that genetic monitoring and screening can invoke requires privacy and data protection legislation, both provincial and federal. Genetic testing raises concerns because of the physical intrusion needed for the collection of genes, as well as the information that it provides. Lori Andrews and Ami Jaeger point out that "the legal permissibility of such disclosures must be assessed against the importance of the protection of confidentiality" (Andrews and Jaeger, 1991:76-77). Issues of confidentiality and intrusion become of great concern when a patchwork legal system provides little protection for employees and individuals, especially in the private sector. The Privacy Commissioner of Canada's 1992 study states that even though "during the study we have found no employment situation that warrants the compulsory or voluntary collection of personal genetic information for the benefit of employers...without compelling arguments to the contrary, genetic screening for the benefit of the employer is inappropriate"

---

[16] The Doman Forest Products Limited Case had to do with surveillance outside of the workplace, but yet perceived to be relevant to work. However, the case is a breakthrough case as it weighs an employee's right to privacy versus the employer's authority. Although this does not mean the employee always wins the case based on an infringement of privacy, but rather, the limits of an employer's powers are subject to review and the potential invasion of privacy is determined on the need for surveillance.

(Privacy Commissioner of Canada, 1992:31).[17]

Genetic screening, with its ability to predict the genetic future of an individual, is a potential privacy danger that needs to be addressed. The day might come when governments and businesses want to test potential employees to "see if they are genetically suited to have access to certain services," or suitable even to be awarded a job (Privacy Commissioner of Canada, 1992:20). The Privacy Commissioner of Canada has suggested that there is a definite need to look into the potential benefits and dangers of genetic testing in both the public and private sectors. The fear of moving towards genetics and genetic control is not a recent one, resulting from work on the Human Genome Project. Twenty-five years ago, Joseph Fletcher pointed out the potential dangers of genetic testing.

> The objection is, predictability, that it would "violate" a "right" - the right to privacy. It is even said, in a brazen attack on reason itself, that we have a "right not to know." Which is more important, the alleged "privacy" or the good of the couple as well as their progeny and society? (in the Privacy Commissioner of Canada, 1992:29).

It is not only a matter of not letting others know one's genetic makeup or predestined genetic future, but also to exercise the right not to know one's own genetic makeup. Thus, a person "should have a right of privacy that protects them from [the] information

---

[17] Although the study found no traces of genetic monitoring, there have been cases of medical monitoring in both the United States and Canada. Lori Andrews and Ami Jaeger point out that "medical screening and monitoring have long been used by employers for a variety of reasons - to exclude people from jobs, to determine whether there is any reason an employee cannot perform the essential functions of a job, to study the workplace's effects on individuals and to target work areas for increased safety and health precautions" (Andrews and Jaeger, 1991:75-76).

that their own bodies can yield" (Privacy Commissioner of Canada, 1992:30). Recommendations made by the Privacy Commissioner of Canada to regulate genetic information include: regulations against mandatory genetic testing, the control of genetic information, and the disclosure of genetic information.

Some legal protection against genetic screening and genetic information can be found under the federal Privacy Act. The Act states that the collection of personal information for the purpose of curiosity is strictly prohibited. The Act "attempts to counter the thirst for information that typifies modern organizations," by regulating the collection of information and the methods of collection. The Privacy Act rules against the collection and disclosure of personal information and this includes information relating to race, ethnic origin, colour and medical history (Privacy Commissioner of Canada, 1992:56). The Privacy Commissioner adds that the definition is broad enough to include the "personal information generated by genetic testing" (Privacy Commissioner, 1992:56). As for the private sector, the Privacy Act, provincial privacy laws and the Charter do not apply, leaving the private sector and its employees susceptible to forms of privacy invasion.[18]

Nonetheless, the use of genetic screening and genetic information in the private and public sectors are still at the infancy stage. This does not mean that the potential consequences of genetic information should be swept under the carpet. Rather, steps

---

[18] It has been mentioned that common law tort concepts can grant employees some protection against privacy invasion, but "whether a common law tort of invasion of privacy exists in Canada remains a subject of debate" (Privacy Commissioner of Canada, 1992:78).

should be taken before hand and the potential invasion of privacy must be addressed. As David Suzuki states, "we must also be willing to play a part in monitoring those who might seek to use discoveries in genetics for personal, political or economic leverage in the endlessly shifting balances of power that are the inevitable consequence of scientific knowledge and its application" (in Privacy Commissioner, 1992:78). The potential dangers of genetic information must be recognized as a threat not only to one individual, at one time, but also to all individuals at all times. There is a need to look at the larger picture when it comes to genetic information (Bennet, 1995).

Genetic information challenges the boundaries of the individual and society and we need to reflect on "how the addition of a genetic profile contributes to the proliferation and multiplication of individual identities within the everyday 'normalization gaze of the Panopticon'" (Bennett, 1995). Genetic information creates an even more in-depth profile of an individual, creating a genetic identity that becomes caught within the gaze, untouchable by its owner but easily used by its collector. Bennett goes on to explain that because of the predictive qualities of genetic information, the potential for in-depth data profiles will increase and regulations meant to deal with the issue of social control and genetics will "shift...away from pragmatic trade-offs toward more fundamental goals" (Bennett, 1995). Privacy fundamentalists include those that are "committed to privacy protection at the expense of other social goals," while it is the privacy pragmatists that are willing to tolerate trade-offs (Bennett, 1995b). Finally, it is necessary to understand not only the qualities of genetic data, but also the boundaries of the legitimacy of the collection of information (Bennett, 1995; Gandy, 1993:132). The "need" for using

genetic information must be weighed against the social issue of privacy in an attempt to question the legitimacy of potential intrusion.

Unions - Dealing with Employee Privacy Invasion

Stepping In When Toes are Being Stepped On

The headlines splash the newspaper articles almost daily it seems with the underlying suggestion that the average employee is under the watchful eye of his/her employer: Quit Watching Me!(Johnson, 1999), Your Boss Is Watching (Evans, 1998), Who's Reading Your E-Mail? (Fitz-James, 1999:E4). Accompanying these tales of privacy violations are the ever changing statistics; the percentages that convince us that the occasional incidence of video surveillance tape or the "once in a lifetime" monitoring of an employee's e-mail is no longer a fact of fiction (irony intended), but rather a factual occurrence. Take note (Example 1) of the small sample of percentages and facts below that are being publicized regarding surveillance and the monitoring of employees.

Example 1

If you work at a major corporation, there's a 45% chance your employer is monitoring your e-mail, voice mail, computer files, phone call or other work-related activities, according to a new report from the American Management Association (AMA) (Diederich, 1999).

Electronic surveillance of employees in Canadian firms has increased sharply over the past few years, according to a senior labour leader (Menezes, 1999).

By the end of the decade, as many as 30 million people may be constantly monitored in their jobs (DeTienne in Mishra:4).

A 1998 American Management Association report, Electronic Monitoring and Surveillance, found that 67% of the organizations (versus 63% in 1997) practice some form of electronic monitoring and surveillance of workplace activities (Williams-Harold, 1999:31).

With the number of monitoring cases seemingly on the rise, it is no surprise that unions in Canada and the United States are angered by the potential for numerous invasions of privacy against their union members. Bear in mind that surveillance and monitoring in the workplace are not new problems as they both have distinct, long-standing histories tied to capitalism, Taylorism, social control, and bureaucracy. But the intensity, continuity and pervasiveness of new forms of monitoring, and the usages of the information collected through monitoring, is what concerns the unions.

The American Telephone and Telegraph (AT&T) company has been monitoring its telephone operators since the late 1800's, although the emphasis of the monitoring has changed in the last 100 years for the "better" in this particular case (Labbs, 1992:101). AT&T now monitors its employees for development purposes, using the information collected to advise operators "what they're doing well, and what they aren't doing so well...but they learn from each other, not just from their bosses" (Labbs, 1992:101).

In addition to the concerns regarding surveillance and the invasion of privacy, unions have also expressed their concerns over the mental and physical effects employees suffer courtesy of workplace monitoring. Various studies by unions both in Canada and the United States have found that workers become stressed out over the pressure of monitoring. In 1990, a study of telecommunication workers done by the University of Wisconsin and the Communication Workers of America Union found "significantly higher levels of depression, extreme anxiety and exhaustion among workers under secret

scrutiny" (Lissy, 1993:20). The study also found symptoms (Example 2) that were linked to workplace monitoring.

Example 2

Physical Symptoms	Percentage
Suffered a loss of feeling in their fingers or wrists.	43% of monitored workers 27% of unmonitored workers
Complained about high tension.	83% of monitored workers 67% of unmonitored workers

Both the International Machinists Union and the Teamsters Union in the United States claimed that the stressful workplace due to electronic monitoring turned the workplace into an electronic sweatshop and that employees were hassled over questions regarding their work procedures (Lissy, 1993:20). Finally, the National Association of Working Women also concluded that workplace monitoring is tremendously stressful on employees, claiming that "the work lives of monitored employees can be characterized by three words: invasion, stress, and fear" (Worsnop in Mishra, 1998). These are only few of the numerous studies that have been done. Ironically, current union aggravation regarding workplace monitoring is focussed on the invasion of privacy more than anything else. The well-being of the worker has been displaced, to some extent, by the well-being of the worker's privacy and the well-being of a worker's personal information. Although privacy remains a human right, it is no longer only the physical and mental consequences of monitoring that the unions are concerned about, but rather how the information collected is being used. Now the concern about surveillance in unions is the worker and

not necessarily the work. The issue of privacy has become an issue of how it hurts its employees legally and psychologically, with the potential effects of surveillance and privacy invasion on work being of secondary concern.

Also, the political, legal, and social issues surrounding workplace monitoring have been shifted, creating a modern concern, the concern for the individual in the form of information. This is not to say that unions do not care about the well-being of their members, but battles regarding workplace privacy in the courts and the government have to do with the information that employees relinquish and generate rather than the employee himself or herself. The employee becomes reduced to productivity quotas, efficiency statistics, time spent working, and keystrokes and not necessarily referred to as an individual who is feeling stress and anxiety because of surveillance methods. The employee, as the subject, gets lost within the battle of privacy, signified as merely a data file that must not get into the wrong hands. However, this argument mainly relates to data protection, and not necessarily the intrusion on privacy. The physical intrusion upon privacy is still a major concern which involves the collection of information. Of course, the employee does not even need to be there. The interception of e-mail or searching e-mail databases does not require any participant to be present. Surveillance can be undertaken without the presence of a participant. Such decentred surveillance is a sign of the times and of the era of new surveillance, distancing the subject, yet engaging it in a machinery of discipline. The employee finds little place to hide inside and outside of the workplace.

One More Video Capture and I Will Tell the Union!

The Canadian Postal Workers Union of Canada (CUPW) has waged some of the more significant battles over the invasion of employee privacy over the last forty years. Dating back to 1956, the CUPW, then known as the Canadian Postal Employees Association, was involved in protests against closed circuit television in the workplace. In the end, the original CCTV experiment failed. However, the issue was not dead. Aside from strikes in 1978 and 1981 that were based partially on the implementation of CCTV devices in the workplace, twenty years after the original attempt of bringing CCTV into the workplace, "postal management embarked on long-range plans to introduce investigative CCTV into 26 major postal facilities across the country as a key part of its technological change worth $1 billion dollars (Hoogers, 1999a).[19] The CUPW waged a successful battle against this intrusion and "negotiated its demise in 1985" (Hoogers, 1999a).

The introduction of CCTV, however, was not the only cause for concern among CUPW members. The mid 1970's, influenced by the overwhelming possibilities of advanced technology, marked the introduction of the electronic monitoring of individual work. Measuring the output of postal workers allowed Canada Post to monitor individual workloads and discipline accordingly. The CUPW took great offence to such an intrusive action and through protests and strikes, successfully eliminated individual work

---

[19] Evert Hoogers is the CUPW's national union representative.

measurement.[20] Unfortunately, the protective clause against such monitoring was lost in the next round of collective bargaining and the union members were forced back to work only to "enshrine the right once and for all in 1980," and "significant arbitration decisions on this clause have occurred in the intervening years" (Hoogers,1999a).[21]

Even to this day, the CUPW continues to protect their members from forms of privacy invasion, although at times their complaints fall on deaf federal ears. Involvement by the Labour Canada Task Force on Microelectronics and Employment in 1982, and a presentation before the House of Commons Standing Committee on Human Rights and the Status of Persons With Disabilities in its hearings on "Privacy Rights and the New Technology" in 1997, are just a couple of the CUPW's efforts in battling employee privacy invasion. In the 1985 Electronic Surveillance Conference of British Columbia Federation of Labour, the president of CUPW stated that "the increasing electronic surveillance of workers is one of the most serious problems facing the trade union movement today" (International Labour Office, 1993a:141). The president went on to suggest that "there was a need for legislation to protect all workers against electronic work measurement and surveillance" (International Labour Office, 1993a:141).

---

[20] Both the Communications Workers of Canada and the Canadian Airline Employees Association were protesting the monitoring of employees along with the CUPW, but they were unsuccessful in their fights against similar electronic individual work measurement (Hoogers, 1999a).

[21] It must be noted that the CUPW collective bargaining agreement provision "prohibits the use of surveillance systems, except to protect against criminal activity" (International Labour Office, 1993a:143). This is still problematic, however, as any form of surveillance intended to capture illegal activity must be properly legitimized; addressing the fact that there is a probable chance of illegal activity being committed by a certain employee or employees.

According to Evert Hoogers, the national union representative, the CUPW has currently "put in a resolution to the upcoming CLC (Canadian Labour Congress) convention calling upon the CLC to lead a campaign for changes to the hodgepodge of so-called privacy legislation across the country focussing on workers' privacy protection" (Hoogers,1999a). The CUPW's appeals to the government for changes in privacy legislation and the removal of some forms of workplace monitoring have gone unnoticed. Hoogers claims that issues such as data protection in the public sector, the protection of medical information, and the need for protection against using information for other purposes needs to be pushed through the government, but the government is slow to respond (Hoogers,1999). Also, collective bargaining provisions are needed to avoid the abuse of employee information. Hoogers also states however that privacy is not on the top of the CUPW list of concerns. Although privacy issues are of considerable importance, they occupy a somewhat different category than wages or seniority protection (Hoogers, 1999b). The CUPW has attempted to halt threats to jobs more than anything else.

Other unions have also picked up the fight against employee privacy invasion issues and the monitoring of employees. The Public Service Alliance of Canada (PSAC) has laid out concerns regarding the medical monitoring and the drug testing of employees. In a PSAC position paper, the union expressed their concern over the medical monitoring of their members, claiming that medical monitoring can be a crude tool used against employees (PSAC Position Paper #2:84). Their concern revolved around the possible implications of medical monitoring, claiming that "as long as medical monitoring is

primarily for the benefit of employers - for minimizing future compensation costs, for eliminating 'susceptible' workers, for detecting affected workers early - it will violate the rights of workers" (PSAC Position Paper #2:85). The union understands the possible benefits of medical monitoring, but unless certain conditions or regulations exist - including that medical tests be scientifically valid, that the tests provide real benefits to the worker, and that there is confidentiality surrounding the information that is revealed - the technology can be viewed as dangerous. The PSAC vows that they will "press for collective agreement language and legislative changes that forces employers to take all necessary measures," to protect the employees and the workplace (PSAC Position Paper #2:88). Similar claims regarding workplace drug testing have also been made by the PSAC. The union opposes all forms of workplace drug testing and will continue to pressure the federal, provincial and territorial governments and to prohibit any sort of drug and alcohol testing in the workplace as well as press for changes to "human rights Acts and the Privacy Act to ensure protection against drug and alcohol testing" (PSAC Position Paper #29:51).

Finally, other unions, such as the Canadian Auto Workers union (CAW), have had their share of problems with surveillance in the workplace. Only recently did CAW catch the Canadian National Railway company collecting and reading employee and union representatives e-mail messages. The CN was also accused of "installing secret video and audio recording devices in an unknown number of workplaces" (CAW Contact, 1998). In response, charges against the CN under the Canadian Labour Code were to be filed and the union claimed that a level of trust and respect had been lost because of CN's intrusion

- a level of trust and respect that have perhaps been lost between many unions, their members, and employers. However, despite this act of privacy invasion and possibly future invasions of worker privacy, CAW does not have a specific policy on workplace surveillance, leaving their workers susceptible to future privacy invasions (Bennett, e-mail correspondence, 1999).[22] As new surveillance technology enters the workplace and current legislation unsuccessfully tries to keep pace, the friction between unions and their employers increases; not only out of hostility, but out of frustration. Legislation is slow to accommodate invasions of privacy and the percentage of employers that use monitoring continues to rise.

It's All About the Bread-and-Butter

With an increase in the use of technology in the workplace and the ongoing threat to privacy, it seems natural that unions would step in and attain some sort of legal understanding. Their members should be ensured some level of privacy protection in the workplace or at least some basic limits regarding the accumulation of personal information. As Urs Gattiker and Dan Paulson point out, "unionism is usually regarded as providing workers with a mechanism for protection against opportunistic behaviour by the employer, while being able to negotiate the conditions needed to facilitate acceptance of and adjustment to the introduction of new office technology" (Gattiker and Paulson,

---

[22] Kathy Bennett is part of the librarian and information systems staff at CAW in Willowdale, Ontario. Our e-mail exchange was brief, consisting of one letter, providing little information other than that stated in the essay.

1999:249). However, as mentioned before, privacy issues do not rank amongst the highest priorities for the unions. As Evert Hoogers points out, privacy and workplace monitoring "are issues of considerable importance, although occupying a somewhat different category than...wages, or seniority rights or the functioning of the grievance procedure" (Hoogers,1999b). He goes on to explain that within Canadian unions, "generally there has not been an overriding concern developed as yet around worker's privacy issues" (Hoogers, 1999b). This is one of the biggest reasons why privacy in the workplace has taken a back seat among the unions - there are other greater concerns. And why not? How can one complain about privacy if that individual does not have a job in the first place? Thus, the bread-and-butter issue is of prime importance when dealing with unions and the issue of workplace privacy.

Employers and union leaders are more prone to protect jobs, rather than deal with technological change and privacy issues per se. Gattiker and Paulson point out that union members and managers "tend to agree that unions should accept technological change if bread-and-butter issues have been safeguarded" (Gattiker and Paulson, 1999:267). It has also been found that union satisfaction is "greatly affected by the union's success in negotiating bread-and-butter issues" (Gattiker and Paulson, 1999:249). The unions, their members, and management end up in a traditional trade-off arrangement, where certain rights, including privacy, are given up in exchange for a paycheck. A study of white-collar employees in Canada revealed that workers feel the unions have some "credibility and bargaining clout in protecting worker's interests," but, payouts and income may "increase organizational allegiance, and thereby positively affect employees' perceptions

about whether a union should accept technology" (Gattiker and Paulson, 1999:270). The larger the payout, the more likely employees will accept technological change. This reasoning is extremely dangerous and can bring undesired consequences to the shop floor employee. The trade off of information and privacy for financial gain due to technological change can be costly in the long run. Employees might not understand, or simply do not want to understand, the implications of privacy invasion, and thus, just follow the wave of technological change. It is hard to argue against a steady income and job security when such "little" sacrifices, such as job monitoring or the collection of personal information, are the consequence. However, as mentioned before, ignorance is *not* bliss, and apathy is no excuse when it comes to the loss of privacy. The basic right of privacy is being eroded when involuntary trade offs are made within the workplace.

These trade offs are no different outside the workplace, either. Most of us give up information in order to receive goods and services. Many of us might even claim that it is "no big deal" or "really of no concern" to lose such an element of privacy. Some might even boldly suggest that the act of giving up information is a voluntary process, and that is where they make their first mistake. It is a mistake to assume that an individual, or even an employee, is part of a voluntary informational process, as information and privacy become a commodity. In order to be a part of the community, part of the workplace, and part of a social network, there is a need to relinquish a degree of freedom. However, a freedom that allows us to fully participate in society is compromised when there is a continuous demand to relinquish information and privacy. An employee loses a degree of freedom in the workplace, when they allow for the monitoring of their work and the

invasion of privacy in return for job security. The employee becomes a cog in the machine, losing individuality in the bureaucratic maze of efficiency. This demand to relinquish an element of privacy becomes a basic extension of managerial social control. Efficiency, the "bottom line", and productivity become the ultimate concerns, and the control of employees, and the lack of control given to employees, through monitoring becomes a crucial factor in maximizing business profitability. As Clement points out, "the close monitoring of employee behaviour represents the logical extension of a dominant management paradigm - pursuit of control over all aspects of the business enterprise" (Clement in Kling, 1996:285).

I am not arguing that the workplace needs to be a free-for-all environment where employees are given unlimited freedoms to guard their privacy at any cost. Rather, I am suggesting that there needs to be a balance between privacy and efficiency. Employee information must be protected, or at least used for a specific, known purpose. The monitoring of employees must be done in an overt fashion and in a manner that does not lay blame on the employee or even single out an employee, but rather is there to help, nurture, and support the employee/employer relationship. Privacy does not necessarily have to be one of the unions' main concerns; it should not, however, be an easy trade off. The trade off should be done on more voluntary and egalitarian terms, and the benefits and costs must be well documented. Management, employees, and unions all must accept the responsibility for privacy, rather than ignoring human and social rights. In addition to accepting responsibility, employees in particular must become aware of the 'trade off' arrangement. Although some studies have shown that people do approve of having their

work monitored (Grant and Higgens in Kling, 1996:287), in general, workplace monitoring brings mixed results. Although monitoring is viewed as a "legitimate but subtle form of managerial intervention...[it can] often backfire when system designers and managers do not pay close attention to people's indirect responses to monitoring" (Grant and Higgens in Kling, 1996). The eagerness to use technology and monitoring in the workplace must be counterbalanced with the issue of rights - privacy rights.

Union Involvement: Participate, Understand, and Focus

Another major problem when it comes to unions and technological change in the workplace, is that unions and their members usually have little opportunity to engage with management to discuss technological change. Technological change[23] will go on with or without the unions, leaving unions and their members no choice but to deal with such a change and its consequences, after the fact. As a result, in many cases unions and employees are left out of the loop when it comes to implementing technological change in the workplace, and it becomes a matter of accepting, or adjusting to, the change. However, merely accepting technological change misses the point. When employees become monitored eight hours a day and personal information becomes easily collected and used by management, unions will go out of their way to protect their employees, especially with the insufficient legal protection found in Canada. Therefore, union track

---

[23] I use the term "technological change" in a most general way to include, automation but also monitoring.

records are blemished by their inability to deal with technological change (Gattiker and Paulson, 1999:271). Union and employment policies will be "aimed at ameliorating the effects, not the process, of most technological change" (Zureik, Mosco and Lochhead, 1987:17).

The main problem, is that management rarely thinks about their employees when implementing monitoring devices and other technological changes. As Rothwell points out, "managers...admitted that they did not really think in these terms [the effect technology had on the work environment] so that such factors would not hardly be seen as criteria for implementing new technology" (Rothwell in Zureik, Mosco and Lochhead, 1987:17). By ignoring the employees, the needs and concerns of the employees are missed. The employees feel that they are an even less significant part of the business and their participation in management decisions is almost non-existent. Thus, the implementation and design of workplace technology is still the majority of the time, "unquestionably managerial prerogatives" (Annette Davis in Zureik, Mosco and Lochhead, 1987:23).

If the process and not the effects of technological change are to be addressed by the unions, there needs to be a cooperative arrangement between management and the unions and ultimately the government. Common goals must be outlined by all parties regarding the needs and consequences of technological change and these goals have to be made clear before its implementation. Unions must also realize that both qualitative and

quantitative bargaining demands must be addressed.[24] A European study on union responses demonstrated that "there was only limited evidence of the development of a qualitative bargaining agenda" (Rigby and Smith, 1999:12). But once again, it is a matter of prioritizing union and employee needs, and qualitative demands take a back seat to financial concerns. In addition to qualitative demands, the European union study also pointed out that trade unions need to be more "responsive to their membership as well as appeal to a wider group of workers and recognise that members have wider needs than those directly associated with the workplace" (Rigby and Smith, 1999:10). The work environment not only includes an employee's production level, but also other factors that are not necessarily work-related that need to be addressed. These factors could also be considered qualitative demands, but they are qualitative demands found off-hours and in the home's of the employees; such as stress and work done after hours.

Finally, it is important for unions not to compromise the employee's physical and psychological well being. Studies in the past, which evaluated monitoring and surveillance in the workplace, tended to focus on the physical effects monitoring had on employees.[25] Although current studies have a similar focus, the focus has shifted towards

---

[24] R. Hyman defines quantitative bargaining demands as "demands covering wages and other financial compensation," while qualitative demands include "the actual conditions of work, the determination of effort levels and the control of production" (in Rigby and Smith, 1999:5). Thus, workplace monitoring, surveillance and employee privacy can be considered a qualitative bargaining demand.

[25] Some studies, as listed by Baarda, are Clement (1984) and DiTecco, Arsenault, and Andre (1992) and a 1992 Bell Canada study performed by CAW. Also, the Privacy Commissioner of Canada's annual reports usually refer to the effects of workplace monitoring on employees and articles by Lissy (1993), and Mishra and Crampton (1998). The Mishra and Crampton article summarizes a variety of individual studies that have

evaluating the potential dangers of privacy invasion and the collection of information through monitoring rather than the physical consequences such as stress and carpal tunnel syndrome (in Mishra and Crampton, 1998:5). However, both the mental and physical effects, and the circumstances surrounding the collection and use of employee information must be addressed. The curbing of surveillance in the workplace thus faces a faceless enemy, that of information. Data, databases, and data profiles become the major concern for unions and employees. Where and how the information is gathered and to what extent privacy is being invaded become the key issues. Therefore, relating back to Priscilla Regan's point, it is the worker that is being focussed on and not the work, and thus it is the information surrendered by the worker that has become even more important (Regan, 1996:21). However, the collection of personal information and the use of that information becomes crucial for management. The worker becomes essentially disassociated from the information he or she relinquishes only to have that information used "against" them in order to create a "perfect worker." Privacy, to a degree, has fallen to the wayside, swept away by the protection of information rather than the protection of the individual. The drive towards efficiency and maximized productivity includes the worker, the work, and information, and all of these components are found within a complex relationship involving surveillance, discipline, and social control. What we are left with is a trade-off relationship between individuals and a social community bent on privacy, and the management "need" to know all. Employees are left to deal with a

---

been conducted over the last six years, including studies on Bell Canada, Federal Express, AT & T, TWA and other independent studies covering various workplaces including a major study by the University of Wisconsin's Department of Industrial Engineering.

complex social relationship based on the paradox of privacy - the loss of privacy and the need for privacy.

Chapter 5 - Conclusion

The issue of surveillance in the workplace has left us in a precarious situation. On the one hand, we still hear the cries of injustice as privacy advocates, high-tech journalists[26], unions, and employees claim that surveillance in the workplace is a definite invasion of privacy. They argue that the workplace merely suffers when employees are surveilled, that surveillance is an infringement of rights and morality, and that the elusive right to privacy is being invaded spearhead their claims. On the other hand, surveillance can be seen as a natural and economic progression, an intensification of what has always been, a need for the control of information to maximize efficiency and maximize employee output. The industrial revolution has lead us to an era dominated by the control, calculation, and tabulation of information. Capitalism and bureaucracy have become part of the reason for the increased intensity of workplace surveillance, but they are pieces of the bigger picture. Economics and administrative control are intertwined with self-discipline, panoptic qualities, information dissemination and separation, and the establishment of an technologically and socially mediated employee/employer relation. Surveillance has become the cause of employee and privacy advocate uneasiness, but it has also produced effects that are simply consequential, secondary in nature, and with relative dangers rather than absolute dangers. The leap to considering workplace surveillance as an absolute danger leads to paranoia and lacks understanding. Thus, there is a need to understand that surveillance is an extension of administrative practices that

---

[26] High-tech journalism is a term coined by Lyon (1994).

have developed in the nation-state, and filtered down to other institutions. Nevertheless, surveillance is also a result of a cultural phenomenon, one where surveillance is needed to deal with both the loss and abundance of privacy (Lyon, 1994).

Employees are needed in the workplace as the survival of the business depends on maximum productivity, efficiency, and the surveillance of employees. Intense surveillance allows for the management of workers but also the management of success through social control. Intensified surveillance in the workplace has in one sense excluded the worker, but in another the worker becomes incorporated into the corporation through some type of monitoring and evaluation.

Also, monitoring goes hand-in-hand with self-discipline and thus employees take on a form of responsibility. Therefore, surveillance becomes a mediator of employer-employee relations, not always invading privacy, but creating an environment where privacy becomes a contextual concept - defined by its boundaries.

However, conceptualizing surveillance and privacy in the workplace does not mean the elimination of the physical or mental consequences of surveillance. The effects of stress, displacement, isolation, and the general concerns of mistrust between employer and employee are real consequences of intense surveillance. But the concept of privacy and its ambiguous inclusion and exclusion parameters is an equally important point when dealing with surveillance in the workplace. The inclusion and exclusion of workers through surveillance is a difficult task to grasp. Workers are monitored and evaluated, and because of this they become part of the company as they become part of the machinery of the workplace. Employees are contributors to the company, efficient

producers, and members of a community. Employees also become involved in the creation of the "perfect worker". This can either mean the moulding of the present worker, or the "weeding out" of the inefficient worker to find the "perfect worker" through surveillance. Workers become identified, regulated, evaluated, and created within the workplace. Finally, employees become involved in the reflexive nature of surveillance. The worker enters a technology of surveillance relationship that includes everyone in the workplace from the top down and back up again.

However, employees also feel excluded because of surveillance. The practice or even threat of surveillance insinuates a level of mistrust. Privacy within the workplace is still a concern because the issue of trust, the ability to voluntarily relinquish information, and the use of information after it has been collected still pose serious problems. How to eliminate these concerns is a difficult issue, but it begins with awareness. Self-awareness of the potential dangers of surveillance *and* the positive aspects of surveillance is a necessary step for employees and privacy advocates. To know why employees are being monitored and surveilled, to understand the social relations of privacy, and to understand that privacy is not always a matter of insuring protection are key ideas that must be addressed.

Methods of workplace surveillance include monitoring of e-mail, genetic screening and video surveillance, all of which are forms of surveillance within the workplace but each characterizes different aspects of surveillance. The monitoring of e-mail solidifies the notion of decentred surveillance within the workplace as the interception of e-mail can be done from anywhere at anytime. The interception of e-mail

also questions the notion of personal property. Video surveillance contains an aspect of prediction, which enables employers to predict employee behaviour and thus justify the use of video cameras as deterrents by forcing the employee to become self-disciplined. Genetic screening also involves the notion of prediction, but it is also a form of self-contained surveillance where the owner of the genes cannot become involved in any form of self-discipline.

From a legal standpoint, the invasion of privacy has become a loud cry for help, but it has fallen on deaf legal ears. In Canadian laws privacy does not qualify as an essential right, thus making it difficult for employees to argue that a violation of privacy is a violation of rights. Ambiguous federal and provincial laws do not facilitate the legal battle for the protection of privacy and for the most part, except Quebec, privacy within the private sector is generally unprotected. Also, the legal system does not always account for the necessity of workplace surveillance or the employer-employee relationship. The boundaries of privacy are unclear in a legal context because privacy extends beyond legality into a social world where the privacy of an employee is negotiated, and the control and use of information are not relegated to simple physical intrusion or protection(Lyon, 1994). Within a legal context, privacy is never clearly defined and current laws fail to address all the aspects of privacy including informational privacy and data protection.

Finally, some unions hold to a bread-and-butter theory that limits how far their pursuits of privacy protection may lead. Such an approach is not inherently bad as privacy concerns become useless if the employee does not have a job to start with. Issues

of privacy are dealt with in two different ways. First, the importance of privacy protection does not always focus on how the employee has become a victim of privacy invasion, but rather the importance of the information collected *about* the employee becomes a major concern. Secondly, the focus of privacy concerns has a tendency to focus on the worker rather than the work. Again, this is not an inherently bad point, but it does illustrate that the boundaries and relations of privacy and privacy concerns are ever changing. Because privacy is complex and ever changing, unions have had to deal, or better yet, are forced to deal with the fact that there is a trade off involved in the workplace between privacy and social control. The multitude of privacy definitions makes the union privacy concerns that much more difficult[27].

The challenge now for the employee is to become involved in a process of awareness; a self-awareness that encompasses a knowledge of the complexities of the social, economic, and bureaucratic elements of privacy. An era of enlightenment is needed, one that will cast a light on the shadow of privacy and on the shadow of the employee. The potentials of surveillance in the workplace must be known, as well as the innate and consequential dangers of a monitored workplace. Without knowing the flexible boundaries of privacy, how can one know what one is fighting for when the threat is unknown? The issue of privacy in the workplace is an important one, and one that deserves attention. But it is a concept, a right, and a relation that becomes disguised behind the over-hyped totality of control. Privacy's undulatory presence should not

---

[27] It must be noted that these findings do not represent all unions, but rather the unions and union cases that were investigated for this thesis.

frighten or discourage privacy advocates, "violated" employees or union representatives. Nevertheless, it should spark debate over what is privacy, and provide a stepping stone for further inquiry. The workplace and its elements of social control, self-discipline, and panoptic properties should represent a fertile ground for the exploration of privacy, one that is just underway. It is a matter of balance and a matter of control by the employee and the employer. The workplace has reached a level of transparency, but it does not mean that everyone is necessarily exposed or violated. Instead, a transparent workplace has the potential to become a clearer workplace, where the employee and employer engage in a relationship of knowledge and trust. But this can only be reached when a balance between useful and useless information is defined, when the employee and even the employer endure a sense of awareness, and when privacy becomes more than just a rallying cry (Schuurman, 1995).

Surveillance in the workplace will continue to increase, there is little doubt about that. But the way in which surveillance is conducted within the workplace must now become a primary concern. Rather than dealing with the consequences of surveillance in the workplace, employees and employers can together be a part of the developmental process. Tech-use policies, e-mail guidelines, union/employer collaboration, and upfront information management practices are a few methods that can be used to deal with intensified workplace surveillance methods.[28]

---

[28] Privacy protection principles for genetic testing (Privacy Commissioner of Canada, 1992) and workplace e-mail privacy (Wright, 1994) have been put forth by various Privacy Commissioners in the past. Some authors, such as Kristen DeTienne and Nelson T. Abbott (1993), also have contributed suggestions towards the development and conceptualization of employee surveillance. DeTienne and Abbott outlined a 7 step

Where unions are not usually present, usually in the white-collar private sector, attempts at educating employees to understand their privacy rights and the passage of adaptable, preventative, and protective oriented legislation should be some of the steps taken in dealing with surveillance related privacy invasion. New legislation should be able to constantly adapt to new technologies, prevent employee privacy invasion, and protect employee data before and after collection.[29] Finally, an attempt at corporate enlightenment is necessary. Educating not only the employees but the employers is needed to instill the notion that privacy is possible to some extent in the workplace. Such a cooperative attitude could also elevate the level of mutual respect between employee and employer. Undertaking the task of employee/employer privacy self-awareness and corporate education is a difficult one, but one that attempts to place the conceptual social definition of privacy back into the hands of the individual. Therefore, there is a great task at hand to embark on a journey towards a cultivated understanding of privacy within the bureaucratically organized, capitalist driven workplace. However, this new found understanding of privacy will not come easily. Exploring the concept of privacy

---

process useful in the designing stage of employee-centred electronic monitoring that included shaping the system to fit the tasks of the users, monitoring only appropriate work related information and a mandatory trial period.

[29] Discussions regarding provincial and federal e-commerce bills, meant to protect online consumer information, have dominated the technology section newspaper headlines for a couple of years now. Other legislation, such as Bill C-6, requires organizations "to allow consumers to opt-in or opt-out of companies collecting information about them" (Mingail, 2000:E2). Slowly, provincial and federal legislation have tried to keep up with the expansion and increasing distribution of personal information. However, the majority of legislation has been aimed at consumers and the private sector and not necessarily employees.

resembles the exploration of an unknown swamp, and while standing on firm ground of what we want to call or what we think is privacy, we sink into the murkiness of its definition (Inness, 1992: 3). But we do not have to sink. Instead we must become involved in the organization and conduct of the workplace, defining ourselves as employees and not data subjects.

Bibliography

A Day in The Life
1997 *Impact.* CNN. June.

Aiello, John R. and Carol M. Svec
1993 "Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence," *Journal of Applied Social Psychology.* 23 (7). Pp. 537-548.

Andrews, Lori B. and Ami S. Jaeger
1991 "Confidentiality of Genetic Information in the Workplace," *American Journal of Law and Medicine.* 17(1 and 2). Pp. 75-108.

Arnaut, Gordon
1996 "Workplace Privacy Becomes a Thorny Issue When Every Move We Make Can Leave a Trail," Globe and Mail. October 22. Pp. C1. gopher://insight.mcmaster.ca:70/0R0-8150-/org/efc/media/globe.22oct96.

Baarda, Carolyn W.
1994a *Computerized Performance Monitoring: Implications for Employers, Employees, and Human Resources Management.* (MIR Thesis) Kingston: Queen's University.

Baarda, Carolyn W.
1994b *Computerized Performance Monitoring: Implications for Employers, Employees, and Human Resources Management.* Kingston: IRC Press.

Beniger, James R.
1986 *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press.

Benn, Stanley I.
1984 Privacy, Freedom, and Respect for Persons," in Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology.* London: Cambridge University Press. Pp. 223-244.

Bennett, Colin
1991 "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," *Science, Technology, & Human Values.* Winter. 16(1). Pp. 51-69.

Bennett, Colin J.
1995 "The Political Economy of Privacy: A Review of the Literature," Final Draft of paper presented to the Center for Social and Legal Research. April. http://www.cous.uvic.ca/poli/bennett/research/gnom.htm..

Bennett, Kathy
1999 CAW Librarian & Information Systems Representative. E-Mail Correspondence, July 26.

Bogard, William
1996 *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge: Cambridge University Press.

Braverman, Harry
1975 *Labor and Monopoly Capital : The Degradation of Work in the Twentieth Century*. New York: Monthly Review Press.

Brin, David
1993 "The Good and the Bad: Outlines of Tomorrow." http://kspace.com/KM/spot.sys/Brin/pages/piece1.html.

Brin, David
1998 *The Transparent Society*. Massachusetts: Addison-Wesley.

Brown, William S.
1996 "Technology, Workplace Privacy and Personhood," *Journal of Business Ethics*. 15. Pp.1237-1248.

Cavoukian, Ann and Don Tapscott
1995 *Who Knows: Safeguarding your Privacy in a Networked World.* Toronto: Random House.

CAW Contact
1998 "CN's Snooping is Unlawful, CAW Charges," *CAW Contact*. April, 28(13).

Chaffey, Douglas Camp
1993 "The Right to Privacy," *Political Science Quarterly*. 108(1). Pp. 117-132.

Clarke, Roger A.
1988 "Information Technology and Dataveillance," *Communications of the ACM*. 31 (5). Pp. 498-512.

Clement, Andrew
1992 "Electronic Workplace Surveillance: Sweatshops and Fishbowls," *The Canadian Journal of Information Science*. December. 17(4). Pp. 18-45.

Cruickshank, Doug
1987 *Electronic Monitoring: A Study of its Effects on Telephone Industry Employees*. MIR Thesis. Kingston: Queen's University.

Cuzzort, R. P. and E. W. King
1989 *Twentieth-Century Social Thought*. Fort Worth: Harcourt Brace Jovanovich College Publishers.

Dandeker, Christopher
1990 *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to Present Day*. Cambridge: Polity Press.

Davies, Simon
1997 "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed From a Right to a Commodity," in Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*. Pp. 143-166.

DeCew, Judith Wagner
1994 "Drug Testing: Balancing Privacy and Public Safety," Hastings Center Report. March-April. 24(2). Pp. 17-23.

DeTienne, Kristen Bell
1993 "Big Brother of Friendly coach," *The Futurist*. September-October. Pp. 33-37.

DeTienne, Kristen Bell and Nelson T. Abbott
1993 "Developing an Employee-Centered Electronic Monitoring System," *Journal of Systems Management*. Pp. 12-15.

Diederich, Tom
1999 "45% of Big Firms Monitor Workers," *CNN*. April 21. http://cnn.com/TECH/computing/9904/21/spyidg.

DiTecco, D., G. Cwitco, A. Arsenault, and M. Andre
1992 "Operator Stress and Monitoring Practices," *Applied Ergonomics*. 28(1). Pp. 29-33.

Ekos Research Associates
1993 *Privacy Revealed: The Canadian Privacy Survey*. Ottawa: Ekos Research Associates.

Evans, Mark
1998 "Your Boss is Watching," *Globe and Mail*. September 17. http://news.globetechnology.com.

Fairweather, N. Ben
1999 "Surveillance in Employment: The Case of Teleworking," *Journal of Business Ethics*. 22. Pp. 39-49.

Fitz-James, Michael
1999 "Who's Reading Your E-Mail?" *The Financial Post*. February 15. E4.

Flaherty, David H.
1997 "Controlling Surveillance: Can Privacy Protection Be Made Effective?" In Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press. Pp. 167-192.

Foucault, Michel
1979 *Discipline and Punish: the Birth of the Prison*. New York: Vintage Books.

Foucault, Michel
1984 *The Foucault Reader*. Paul Rabinow (ed.) New York: Pantheon Books.

Fried, Charles
1984 "Privacy [A Moral Analysis]," in Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*. London: Cambridge University Press. Pp. 203-222.

Gandy, Oscar H. Jr.
1993 *The Panoptic Sort*. Boulder: Westview Press.

Gandy, Oscar H. Jr.
1989 "The Surveillance Society: Information Technology and Bureaucratic Control," *Journal of Communication*. 39(3). Pp. 61-76.

Garson, Barbara
1989 *The Electronic Sweatshop: How Computers are Transforming the Office of the Future into the Factory of the Past*. New York: Penguin Books.

Gattiker, Urs E. and Dan Paulson
1999 "Unions and New Office Technology," Relations Industrielles/Industrial Relations. 54(2). Pp. 245-276.

Giddens, Anthony
1995 *A Contemporary Critique of Historical Materialism.* London: The Macmillan Press Ltd.

Giddens, Anthony
1987 *Social Theory and Modern Sociology.* Stanford: Stanford University Press.

Giddens, Anthony
1990 *The Consequences of Modernity.* California: Stanford University Press.

Giddens, Anthony
1993 *The Giddens Reader.* (ed.) Philip Cassell. London: The Macmillan Press Ltd.

Giddens, Anthony
1985 *The Nation-State and Violence.* Los Angeles: University of California Press.

Gilliom, John
1994 *Surveillance, Privacy, and the Law: Employee Drug Testing and the Politics of Social Control.* Ann Arbour: The University of Michigan Press.

Goffman, Erving
1961 *Encounters.* New York: The Bobbs-Merrill Company Inc.

Goffman, Erving
1959 *The Presentation of Self in Everyday Life.* New York: Anchor Books/Doubleday

Gotlieb, C.C.
1996 "Privacy: A Concept Whose Time Has Come and Gone," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press. Pp. 156-174.

Harowitz, Sherry L.
1998 "E-Mail's Packet of Problems," *Security Management.* Pp. 47-54. 42(10).

Hecker, Steven and Mark S. Kaplan
1989 "Workplace Drug Testing as Social Control," *International Journal of Health Services.* 19(4). Pp. 693-707.

Hoogers, Evert
1999a CUPW's National Union Representative. E-Mail Correspondence, February 22.

Hoogers, Evert
1999b CUPW's National Union Representative. E-mail Correspondence, August 6.

Hoogers, Evert
1999 CUPW's National Union Representative. Telephone Correspondence, July.

House of Commons Standing Committee
1997 *Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities.* http://www.parl.gc.ca/committee352/huso/reports/03_1997-04/huso-03-cov-e.html.

Inness, Julie C.
1992 *Privacy, Intimacy and Isolation.* New York: Oxford University Press.

International Labour Office
1993a "Worker's Privacy, Part II: Monitoring and Surveillance in the Workplace," *Conditions of Work Digest.* Geneva: International Labour Office. Volume 12(1).

International Labour Office
1993b "Worker's Privacy, Part III: Testing in the Workplace," *Conditions of Work Digest.* Geneva: International Labour Office. Volume 12 (2).

Johnson, Tracy
1999 "Quit Watching Me!" *Globe and Mail.* January 29. http://news.globetechnology.com.

Kling, Rob and Jonathan P. Allen
1996 "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press. Pp. 104-131.

Laabs, J.J
1992 "AT&T's Self-Monitored Work Teams," *Personnel Journal.* Pp.101. June.

Lawson, Ian and revised by Bill Jeffery
1997 *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector.* Ottawa: The Public Advocacy Centre.

Lewis, Len
1997 "Big Brother is Watching," *Progressive Grocer.* February. 76(2). Pp. 22-28.

Lind, Laura
1998 "Messages that Bite Back," *The Financial Post.* August 15-17. Pp. IT11.

Lissy, William E.
1993 "Surveillance of Workers," *Supervision.* 54(2) Pp. 20.

Luborsky, Gordon F. and John C. O'Reilly
1997 *Employee Surveillance: Defining the Boundaries.* Scarborough: Carswell.

Lyon, David and Elia Zureik
1996 "Surveillance, Privacy, and the New Technology," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press.

Lyon, David
1994 *The Electronic Eye: The Rise of Surveillance Society.* Minneapolis: University of Minnesota Press.

Lyon, David
1988 *The Information Society: Issues and Illusions.* Cambridge: Polity Press.

Mainprize, Steven
1996 *Elective Affinities in the Engineering of Social Control: The Evolution of Electronic Monitoring.* http://www.sociology.org/vol002.002/Mainprize.article.1996.html.

Manes, Stephen
---- "How Much Privacy Do You Really Want?" *PC World Online.* http://www.idg.net/go.cgi?id=35659.

Martin, Sandra
1999 "Vital Signs: Oh Pity our Ever-Shrinking Private Parts," *Globe and Mail.* April 10. http://news.globetechnology.com.

Marx, Gary T. and Sanford Sherizen
1986 "Monitoring on the Job: How to Protect Privacy as well as Property," *Technology Review.* November/December. Pp. 63-72.

McLean, Deckle
1995 *Privacy and its Invasion.* Connecticut: Praeger.

Menezes, Joaquim
1999 "More Employers Spy on Workers: Electronic Surveillance of Employees is on the Rise, and One Labour Leader Says it Makes Work Stressful," *Computing Canada.* June 11. 25(23). Pp. 11-13.

Mingail, Sandra
2000 "Data-Mining, Privacy: Oil and Water?" *The National Post.* January 24. E2.

Mishra, Jitendra M. and Suzanne M. Crampton
1998 "Employee Monitoring: Privacy in the Workplace," *S.A.M. Advanced Management Journal*. Summer. 63(3). Pp. 4-14.

Mowshowitz, Abbe
1996 "Social Control and the Network Marketplace," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press. Pp. 79-103.

Murphy, Robert F.
1984 "Social Distance and the Veil," in Ferdinand David Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*. London: Cambridge University Press. Pp. 34-55.

Nebeker, Delbert M. and B. Charles Tatum
1993 "The Effects of Computer Monitoring, Standards, and Rewards on work Performance, Job Satisfaction, and Stress," *Journal of Applied Social Psychology*. 23(7). Pp. 508-536.

Nock, David
1993 *The Costs of Privacy: Surveillance and Reputation in America*. New York: Aldine de Gruyter.

Ontario Law Reform Commission
1996 *Report on Genetic Testing*. Toronto.

Pedeliski, Theodore B.
1997 "Privacy and the Workplace: Technology and Public Employment," *Public Personnel Management*. Winter. 26(4). Pp. 515-527.

Perrolle, Judith A.
1996 "Privacy and Surveillance in Computer-Supported Cooperative Work," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press. Pp. 47-65.

Phillips, Bruce
1998 *Privacy Commissioner, 1997-1998 Annual Report*. Ottawa.

Plummer, David
1998 "Surviving the Workplace," *ABC News*. http://more.abcnews.go.com/sections/us /work/work_surviving.html.

Poster, Mark
1990 *The Mode of Information: Poststructuralism and the Social Context.* Cambridge: Polity Press.

Poster, Mark
1995 *The Second Media Age.* Cambridge: Polity Press.

Pringle, Matti and Paul Edwards
1995 *Donkeys in the Age of Smart Machines: A Case Study of Electronic Control and Worker Responses.* Coventry: University of Warwick.

Privacy Commissioner of Canada
1992 *Genetic Testing and Privacy.* Ministry of Supply and Services: Ottawa.

Privacy Commissioner of Canada
1998 Study Extracts. http://privcom.gc.ca/study.htm.

Privacy Committee of New South Wales
1995 *Invisible Eyes: Report on Video Surveillance in the Workplace.* http://www.austlii.edu.au/au/other/privacy/video/index.html.

PSAC
---- PSAC Position Paper #2. http://www.psac.com/COMM/POLICY/pos2e.pdf.

PSAC
---- PSAC Position Paper #29. http://www.psac.com/COMM/POLICY/pos29e.pdf.

Regan, Priscilla
1996 "Genetic Testing and Workplace Surveillance: Implications for Privacy," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press. Pp. 21-46.

Regan, Priscilla
1993 "Ideas or Interests: Privacy in Electronic Communications," *Policy Studies Journal.* 21(3). Pp. 450-469.

Rigby, Mike and Roger Smith
1999 "Union Responses in Electronics: A Globalised Environment," Industrial Relations Journal. 30(1). Pp. 2-15.

Rosenberg, Richard
1997 The Social Impact of Computers. San Diego: Academic Press.

Ross-Pederson, Cynthia
1997 "Difference Between Monitoring, Spying," *Computing Canada*. January 20. 23(2). Pp.9.

Rule, James B.
1996 "High-Tech Workplace Surveillance; What's Really New," in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press. Pp. 66-78.

Rule, James B.
1973 *Private Lives and Public Surveillance*. London: Allan Lane.

Schuurman, Peter J.
1995 *Spying, Peeping and Watching Over: The Beguiling Eyes of Video Surveillance*. Sociology Master of Arts Thesis. Queen's University.

Selling the Future
1994 *Visions of Heaven and Hell*. Part 1 of 3. Barraclough Carey production for Channel 4.

Sewell, Graham
1996 "Be Seeing You: A Rejoinder to Webster and Robins and to Jenkins," *Sociology*. 50(4). Pp. 785-797.

Shaiken, Harley
1984 *Work Transformed: Automation and Labor in the Computer Age*. New York: Holt, Rinehart and Winston.

Simitis, Spiros
1987 "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review*. 135. Pp. 707-746.

Smith, H. Jeff
1994 *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: The University of North Carolina Press.

Staples, William G.
1997 *The Culture of Surveillance: Discipline and Social Control in the United States*. New York: St. Martin's Press.

Task Force on Electronic Commerce, Industry Canada, Justice Canada
1998 *The Protection of Personal Information: Building Canada's Information Economy*. Ottawa.

Thompson, E.P.
1963 *The Making of the English Working Class.* London: Victor Gollancz Ltd.

Tucker Jr., Kenneth H.
1998 *Anthony Giddens and Modern Social Theory.* London: Sage Publications

US Department of Labor, Department of Health and Human Services, Equal Employment Opportunity Commission
1998 *Genetic Information and the Workplace.* http://www.dol.gov/dol/_sec/public/media/reports/genetics.htm.

Warren, Samuel D., and Louis D. Brandeis
1893 "The Right To Privacy," *Harvard Law Review.* December 15(4). Pp.193-220.

Weber, Max
1963 *Max Weber.* S. M. Miller (ed.). New York: Thomas Y. Crowell.

Weber, Max
1930 *The Protestant Ethic and the Spirit of Capitalism.* London: Routledge.

Webster, Frank
1995 *Theories of the Information Society.* New York: Routledge Press.

Wessells, Michael G.
1990 *Computer, Self, and Society.* New Jersey: Prentice Hall.

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

Whalen, John
1995 "You're Not Paranoid: They Really Are Watching You," *Hotwired*, March. Pp. 1-7, http://www.wired.com/collections/privacy/3.03_security_tech1.html.

Whitaker, Reg
1999 *The End of Privacy: How Total Surveillance is Becoming a Reality.* New York: The New Press.

Who's Watching Whom?
1998 *The National Magazine.* CBC. May 18.

Williams-Harold, Bevolyn
1999 "Big Brother Works 9 to 5," *Black Enterprise.* March. 29(8). Pp. 31.

Wolfe, Alan
1997 "Public and Private in Theory and Practice: Some Implications of an Uncertain Boundary." in Jeff Weintraub and Krishan Kumar (eds.), *Public and Private in Thought and Practice.* Chicago: The University of Chicago Press. Pp. 182-203.

Wright, Tom - Information and Privacy Commissioner of Ontario
1994 *Privacy Protection Principles for Electronic Mail Systems.* Ottawa.

Wright, Tom - Information and Privacy Commissioner of Ontario
1993 *Workplace Privacy: The Need for a Safety-Net.* http://www.ipc.on.ca/Web_site.ups/Intro/Frames.htm.

Zuboff, Shoshana
1988 *In the Age of the Smart Machine: The Future of Work and Power.* New York: Basic Books.

Zureik, Elia, Vincent Mosco and Clarence Lochhead
1987 *Telephone Workers' Perception of Management Strategy and Union Reaction to the New Technology.* Kingston: Industrial Relation Centre, Queen's University.