(Be)Labouring the Subject:
Employee E-Mail Surveillance and
the Limits of Surveillance Theory

by

Sandra D. Kahale
B.A. (Honours), University of Western Ontario, 1993

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF ARTS

in the Department of Political Science

We accept this thesis as conforming to
the required standard

[redacted]

Dr. Colin J. Bennett, Supervisor (Department of Political Science)

[redacted]

Dr. R.B.J. Walker, Departmental Member (Department of Political Science)

[redacted]

Dr. Rebecca Grant, Outside Member (Faculty of Business)

[redacted]

Dr. David H. Flaherty, External Examiner (Department of History, University of Western Ontario)

University of Victoria

Supervisor: Dr. Colin J. Bennett

ABSTRACT

Surveillance is arguably one of the central features of modernity. In general terms, the literatures on surveillance have tended to frame the problem as one of law, technology, or sociology. This thesis traces how surveillance has been problematized by these literatures, and outlines how each has contextualized, accounted for, and theorized emerging patterns of surveillance, focusing specifically on the practice of employee e-mail monitoring. In doing so, it builds the case that certain issues that are central to understanding what surveillance is and what it does have been largely ignored by the literature. In particular, it makes the point that contemporary surveillance theory fails to account for or consider the effects of surveillance on subjectivity. The thesis concludes by arguing that the literature on surveillance would be tremendously enriched by a consideration of some of the themes which have preoccupied post-structuralists.

[redacted]

Dr. Colin J. Bennett, Supervisor (Department of Political Science)

[redacted]

Dr. R.B.J. Walker, Departmental Member (Department of Political Science)

[redacted]

Dr. Rebecca Grant, Outside Member (Faculty of Business)

[redacted]

Dr. David H. Flaherty, External Examiner (Department of History, University of Western Ontario)

Table Of Contents

ACKNOWLEDGMENTS

This has been a long, long journey, and I am pleased to have finally reached the end of it. Along the way, many people have contributed emotional and intellectual support, and showered me with little acts of kindness. These, perhaps more than the final product, have made the journey worthwhile...

My deepest thanks go to Geoff Rempel, who had the wisdom not to ask me too often how things were going and who was my refuge from the storm, which I appreciate more than he'll ever know. My sincere thanks also go to Mingus, a charming young adventurer who has been my most constant companion along the way.

My eternal thanks also to my parents, who have supported me emotionally and financially throughout this project, as always.

My thanks to Steen Hume and Debbie Lisle, and also to Peter Nyers. I'm glad we could share this journey together.

I am also extremely grateful to David Flaherty, who sparked my interest in privacy and surveillance issues, and who has been extremely generous to me in countless ways. My thanks also to his excellent staff at the Office of the Information and Privacy Commissioner for the Province of British Columbia.

My most sincere thanks also go to Colin Bennett, whose patience, guidance and support have been greatly appreciated. Thanks also to R.B.J. Walker and Rebecca Grant, who have been kind enough to serve on my committee.

Sandra Kahale
Toronto, 1996

Introduction: Discourses of Surveillance

As we near the end of the twentieth century, surveillance seems to be becoming an increasingly inescapable feature of life in the emerging information economies of the West. Technological innovations and improvements over the past few decades have arguably contributed to the growth of surveillance by making it easier, more affordable, and less visible than ever before. In particular, the computerization of many of the transactions that we engage in on a daily basis has created the potential for detailed electronic profiles to be constructed using the data trails left behind whenever we engage in such transactions. These profiles are compiled and used by various organizations for any number of purposes, often without people ever being aware of the "ways in which their lives are being monitored, and without there necessarily being any evil design on the part of those who do the monitoring."[1] In this context, surveillance is increasingly experienced as the "mundane, ordinary, taken-for-granted world of getting money from a bank machine, making a phone call, applying for sickness benefits, driving a car, using a credit card, receiving junk mail, picking up books from the library, or crossing a border on trips abroad."[2] When we engage in these activities, we leave behind, or may potentially leave behind, electronic footsteps. Thus, as David Lyon comments, "to participate in modern society is to be under electronic surveillance."[3]

In a modern context, surveillance can be understood as "the systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates."[4] Some writers on this theme have found it useful to attempt to distinguish between surveillance and monitoring as involving two different kinds of practices. Thus, one source notes that "monitoring is referred to when it is in

---

[1] Robert Holmes, *Privacy: Philosophical Foundations and Moral Dilemma's*, in Privacy Disputed. Pieter Ippel, Gaus de Heij and Bart Crouwers, ed. (The Hague: Registratiekamer, 1995) pp. 67.
[2] David Lyon, The Electronic Eye: The Rise of Surveillance Society. (Minneapolis: University of Minnesota Press, 1994) pp. 4.
[3] Ibid.
[4] Roger A. Clarke, *Information Technology and Dataveillance,* in C. Dunlop and R. Kling, eds. Computerization and Controversy. (Academic Press, 1991), pp. 497.

relation to performance, while surveillance implies observation of activities, often secretly."[5] In some cases, then, the term monitoring is reserved for the kinds of patterns of surveillance that have come to characterize the workplace. Such distinctions, however, are often tenuous, and generally serve to blur the larger social patterns that both surveillance and monitoring practices participate in and produce. For certainly monitoring, like surveillance, involves the collection of information with the intention of using that information to exert some form of control.[6] From this perspective, the method of collection, or the ostensible reasons for collection, are not particularly relevant, and constitute an artificial distinction between monitoring and surveillance. Thus it is not surprising to find that there is ultimately a great deal of overlap in how the terms are used in the literature. My use of the terms interchangeably here reflects this larger pattern within the literature.

The extension of surveillance in a contemporary context indicates, in part, the commodification of information and the connected expansion of the fields of telecommunications and computers. This has given rise to the concept of dataveillance, which refers quite simply to the use of personal data and personal data systems as a component of surveillance techniques.[7] A related and equally significant factor has been the changing nature of work, which has reflected the widespread expansion of these technologies. As a variety of work tasks have been computerized, opportunities for electronic monitoring have abounded. A study conducted by the United State's Congress Office of Technology Assessment identified the office jobs that were most likely to be subject to electronic monitoring as: word processors, data-entry clerks, telephone operators, customer service representatives, telemarketers, insurance claims clerks, mail clerks, and bank proof clerks.[8] The study also noted that, in most cases, the jobs that were most likely to

---

[5] Michele Jankanish, *Monitoring and surveillance in the workplace: Privacy issues in an international perspective*, in Conditions of Work Digest. Volume 12, Number 1, 1993; pp. 12.
[6] James B. Rule, D. McAdam, L. Stearns and D. Uglow. *Documentary Identification and Mass Surveillance in the United States*, Social Problems 31 (December 1983): 223 as quoted in David H. Flaherty. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, & The United States. (Chapel Hill and London: The University of North Carolina Press, 1989), pp. 409.
[7] See Clarke, pp. 498.
[8] United States Congress, Office of Technology Assessment (OTA), The Electronic Supervisor: New technology, new tensions. OTA-CIT-333. (Washington, D.C.: U.S. Government Printing Office, 1987), pp. 29.

be monitored involved a limited number of standardized tasks which were performed repeatedly and produced an information-based product. "Monitored jobs also tend to be those subject to a work measurement system, whereby the employer has set a standard of performance and measures actual performance against the standard."[9]

The apparent growth of surveillance, and of electronic surveillance more particularly, has been accompanied by a diffusion of surveillance power. Traditionally, surveillance has been the prerogative of the state and, more particularly, of law enforcement agencies. In modern societies, however, surveillance has increasingly become associated with a wide variety of organizations which include, but are not limited to, businesses, charities, providers of various services, educational institutions, governments, and hospitals. The erosion of the role of the state as the sole legitimate agent of surveillance and the subsequent spread of surveillance technologies through other institutions are features of the growth of what some critics have called "surveillance societies."[10]

Surveillance societies are characterized by the existence of automated data bases which facilitate "systematic attention to a person's life aimed at exerting influence over it."[11] In such societies, surveillance functions as a *strategy of power* which operates by enabling its agents to identify and classify subjects as citizens, students, workers, consumers, or users of various services. This process of identification and classification in turn allows governments, businesses, advertising executives, and others to exert increasingly more precise and effective control over those subjects and their behaviours.[12]

The large and growing place of surveillance in modern societies raises a host of important questions, some of which have been addressed in various ways by the

---

[9] Jankanish, op. cit., pp. 16.

[10] See Flaherty, pp. 1-17 and Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order. (Great Britain: Pan Books, 1996). Data protection legislation in this country reflects anxiety around the government's traditional role as the principal site of surveillance; in all provinces except Quebec, only government data bases are covered by such legislation. The recent announcement that Canada will have private sector privacy legislation in place by the year 2000 reflects the growing awareness that surveillance power has been shifting to the private sector over the past decade.

[11] Rule et al., *Documentary Identification and Mass Surveillance in the United States*, in Flaherty, pp. 409.

[12] This is the theme of Oscar Gandy, Jr's , The Panoptic Sort: A Political Economy of Personal Information. (Colorado: Westview Press, 1993).

rapidly expanding literature on this topic. This literature has tended to reflect three principal approaches to the study of surveillance: the legalistic, the technological, and the sociological. Together, these three axes have marked the discursive boundaries of contemporary surveillance theory, not only enclosing debates about surveillance, but also delimiting the parameters of resistance.

In general terms, then, the literatures on surveillance have tended to focus on particular types, instances, or technologies of surveillance as problems of law, technology, or sociology. While each of the literatures has had its own preoccupations, the apparent growth of surveillance in recent decades has brought the question of limits to the forefront in all of them. The availability of increasingly invasive technologies of surveillance has forced the various literatures to grapple with the question of how much surveillance we, as a society, can or will tolerate. Such questions are clearly important and increasingly pressing, given the apparent relentlessness with which new surveillance technologies are being developed and used. Nevertheless, it is not my intention here to engage in a debate about how much surveillance is too much. Rather, I want to suggest that this debate is in some ways beside the point, and that, more significantly, it has marginalized issues that I take to be central to understanding what surveillance is and what it does. Thus, while surveillance is clearly an instance of the functioning of power, it has largely escaped political analysis.[13] Part of my project here, then, it to address some of the political issues around surveillance.

More specifically, I want to suggest that while the debate around the acceptable limits of surveillance is an interesting one, it is perhaps less interesting than the limits of the debate around surveillance more generally. In particular, I am interested in how the parameters of that debate have been circumscribed by the lack of dialogue among the technological, sociological, and legalistic literatures on

---

[13] There are some notable exceptions here. See, for example, Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States. (Ithaca and London: Cornell University Press, 1992); Charles Raab, *Protecting Privacy Across Borders*, Public Administration. Spring 1994, Volume 72, and *Open Government: Policy Information and Information Policy*. Political Quarterly, Jul-Sept. 1994, Volume 65; and Priscilla Regan, Legislating Privacy: Technology, Social Values and Public Policy. (Chapel Hill: University of North Carolina Press, 1995). Bennett, Raab, and Regan have provided some political analyses of surveillance and privacy issues, but their efforts have had uneven success in terms of their impact on larger debates around these issues.

surveillance. These three approaches have emerged as parallel discursive universes within the literature, developing alongside one another, but not engaging each another in any meaningful or sustained way. So while one of my goals here is to interrogate each of these approaches in terms of the contributions it makes, or might make, to understanding surveillance, my interest in the particulars of each approach is really only a peripheral one. My real concern is instead with the *silences* that exist between these discourses, for these silences speak volumes about the work that remains to be done in this field. At the same time, they provide critical insight into the assumptions that underlie much of the work on surveillance. Thus my goal is to consider not only the work that *is* being done, but also some of the work that is *not* being done and cannot be done within the present parameters of the discourse. In essence, then, I am interested in teasing out what these silences have meant for the development of theories that attempt to account for or explain surveillance, and also for the elaboration of strategies of resistance.

Throughout this project, my principal interest is in the ways that contemporary surveillance theory accounts for, or fails to account for, the effects of surveillance on subjectivities. Here I draw from the theme, developed in what is broadly referred to as post-structuralist literature, that subjects are constituted through acts and structures of communication. My reading of surveillance suggests that it can be understood as one component of those structures. Thus I argue that there are important insights to be gained from a meeting of post-structuralism and the literatures on surveillance. To date, such meetings have taken place only in small and relatively isolated pockets. So I conclude this paper by exploring some of the ramifications of a more sustained interaction between these literatures.

Since surveillance practices do not lend themselves to generalizations, sweeping or otherwise, I have chosen workplace surveillance, and in particular the emerging practice of monitoring employee electronic mail (e-mail), to carry my reading of surveillance theories, and of the discourse of surveillance more generally. I have done this in spite of recent criticisms from some analysts that the concern over workplace surveillance is exaggerated, and does not correspond to either the

incidence or the severity of actual practices.[14] Such criticisms may indeed be well-founded, but the *potential* for extensive and intrusive surveillance in the workplace has been clearly demonstrated, and it this potential that makes workplace surveillance useful as a test of the limits of current theories of surveillance. Thus I do not attempt to build the case that employee e-mail monitoring is prevalent, but rather work from the premise that it is exists as a practice, and that this very existence raises important and interesting questions about surveillance, politics, and society.

Another reason for focusing on an instance of workplace surveillance is that, in most cases, employers or managers have a clear interest in shaping employees into particular kinds of (disciplined) subjects as a means to achieving maximum profitability. Surveillance, I argue, has been one way of achieving this goal. The disciplinary aspects of surveillance are, in my opinion, of tremendous political and social significance. An analysis of a workplace surveillance practice, such as employee e-mail monitoring, provides a framework through which to consider how structures of power in the workplace are produced and reproduced through surveillance. Here the relationship between power and surveillance is made explicit, and the extent to which surveillance plays a role in maintaining pre-existing distributions of power, both in the workplace and in society more broadly, is highlighted.

A third and related reason for focusing on workplace surveillance is that it allows me to address the relationship between surveillance and discrimination along gendered, racial, and class lines. Studies show that the jobs that provide the conditions most amenable to surveillance are those that tend to be dominated by women, racial and ethnic minorities, and lower-paid workers.[15] Thus an example of surveillance which is drawn from the workplace provides a good framework through which to consider how surveillance functions differently among different segments of the population, and to contemplate its broader relationship to social order.

---

[14] See James Rule, *High-Tech Workplace Surveillance: What's Really New?* in David Lyon and Elia Zureik, (Eds.) Computers, Surveillance and Privacy. (Minneapolis/London: University of Minnesota Press, 1996).

[15] Spiros Simitis, "Developments in the Protection of Workers' Personal Data" in Conditions of Work Digest: Workers' Privacy, Part 1. (Geneva: International Labour Office, 1991) pp. 12.

A final reason for focusing on a workplace surveillance practice is that, although some critics would argue that we are in a period of transition where consumption is replacing production as the primary signifier of social status in the West, employment continues to occupy an extremely important place in our lives, providing not only social status, but also a sense of identity.[16] Thus it seems particularly important to consider what theories of surveillance can tell us about whether and how surveillance in the workplace changes our experience of being workers.

The modern workplace, with its various sophisticated instruments of work, is the site of a wide range of surveillance practices. These include, for example, key stroke monitoring, drug testing, video surveillance, random or continuous telephone surveillance, computerized workstation monitoring, and the use of access cards or other devices to monitor the whereabouts of employees. While each of these practices raises important questions about surveillance, and about the relationship between surveillance and subjectivity, I find the emerging issue of employee e-mail monitoring especially interesting for a number of reasons. First, as a form of surveillance which is certainly new and quite possibly growing, the monitoring of e-mail in the workplace has not yet received as much attention in the literature as some of these other forms of surveillance. Thus little has been written about the larger social implications of e-mail surveillance. Second, many people presently have access to e-mail only through their workplaces. Their e-mail accounts provide them with access to the Internet, which is becoming an important site for emerging forms of social interaction and new configurations of the relationship between identity and subjectivity. The growing importance of the Internet gives a certain urgency to questions about what it means to engage in these new social forms under conditions of surveillance. A consideration of employee e-mail surveillance, then, provides a forum in which to ask whether such surveillance is inscribing the new social space of the Internet with old social relations, and what the implications of this might be.

---

[16] On this and related themes see, for example, Theodor Adorno, The Culture Industry. (New York and London: Routledge, 1992), Jean Baudrillard, The Ecstasy of Communication. (New York: Semiotext(e), 1987) and For a Critique of the Political Economy of the Sign. (St. Louis: Telos Press, 1981), Zygmunt Bauman, Freedom. (Minneapolis: University of Minnesota Press, 1988) and Intimations of Postmodernity. (New York and London: Routledge, 1992).

Since a substantial part of my project here involves an analysis of the discourse around employee e-mail monitoring, and around surveillance more generally, I begin this paper by considering the parameters of public discussion around the issue of monitoring employee e-mail. The purpose of Chapter One is essentially twofold: first, to provide a profile of current monitoring practices with regards to employee e-mail, and second, to trace the discourse around these practices as it has unfolded in public arenas through mediums such as newspaper and magazine articles, political debates, statements from privacy officials, and debates on and about the Internet. Here I consider what aspects of surveillance have been problematized and by whom, and what kinds of solutions have been proposed to address these problems.

In the second chapter, I move away from the specifics of employee e-mail surveillance to consider the place of this practice, and of workplace surveillance more generally, within larger structures of surveillance. Here I use the works of theorists who have played a foundational role in surveillance theory, including Max Weber, Karl Marx, and Michel Foucault, to sketch the historical context within which contemporary surveillance societies have emerged, and to point to the directions in which they have evolved. In doing so, I situate surveillance as a specifically modern phenomenon, and consider the works of theorists, like Anthony Giddens, who have attempted to make sense of the relationship between surveillance and modernity.

The second chapter, then, outlines the larger context within which particular workplace surveillance practices have emerged in order to demonstrate how the larger social patterns that are associated with surveillance are produced and reproduced in the specific case of e-mail monitoring. Outlining the larger context in which contemporary surveillance practices have emerged also allows me to highlight what has been understood to be at stake in current debates around surveillance, and to trace how such understandings have been arrived at. Throughout the chapter, then, I am particularly interested in teasing out how assumptions about the nature and function of surveillance have been filtered through the approaches of the foundational theorists into contemporary surveillance theory.

In Chapter Three, I move away from the more generalized conceptualization of surveillance as a feature of modernity to consider the particular ways in which

contemporary surveillance practices have been understood from a theoretical perspective. Here I consider the lines along which this literature has developed, paying particular attention to whether and how it has articulated and accounted for the larger patterns of surveillance which are traced in Chapter Two. In sketching the development of this literature, I pay particular attention to the three principal axes along which understandings of contemporary surveillance practices have developed -- the legalistic, technological, and sociological -- and consider the themes which have predominated in each of these literatures. I am also interested here in teasing out the often unspoken assumptions that have given rise to particular framings of the issues in debates about surveillance.

At the end of the third chapter, I return to the particular case of employee e-mail monitoring and consider what the legalistic, technological, and sociological literatures on surveillance can tell us about this practice. Building on the case made throughout this chapter that there has been a lack of meaningful cross-fertilization among the surveillance literatures, I indicate areas where such cross-fertilization might lead to a clearer or more profound understanding of the nature and functions of employee e-mail surveillance, and of surveillance more generally.

In the final chapter, I conclude by arguing that, even though cross-fertilization among the legalistic, technological, and sociological literatures would be an important first step in gaining a better understanding of the issues raised by employee e-mail surveillance, there are still some issues that are not being or cannot be addressed within the present parameters of the debate. In particular, I argue that, by and large, the discourse of surveillance has failed to take seriously questions about subjectivity. Reviewing the conclusions of the previous chapters, I suggest that the literature on surveillance would by greatly enriched by drawing upon other literatures where the theme of subjectivity has figured more prominently. More specifically, I argue that an intersection of post-structuralist and surveillance theories would likely yield useful insights into the role that surveillance plays in enabling, constraining, or manipulating subjectivities, and I consider what the ramifications of this intersection might be for a politics of counter-surveillance. Finally, I consider why it is that such an intersection has generally not occurred or has occurred only on the periphery of the literature on surveillance.

Chapter One: Profile of a Workplace Surveillance Practice

As we near the end of the twentieth century, electronic mail is becoming an increasingly indispensable tool in the workplace. The Electronic Messaging Association, which represents 400 leading e-mail technology firms, estimates that use of e-mail in the business sector grew from one million in 1984 to 16 million in 1993.[1] By that time, business users were sending an estimated five or six billion messages a year. A study conducted by the International Data Corporation in Massachusetts shows that "at least a portion of the workforce at every Fortune 500 company uses e-mail, while only 80 percent of the companies have installed voice-mail systems."[2] E-mail, then, is clearly becoming an important form of business communication.

In this chapter, I trace the growing importance of e-mail in the workplace, and examine the nature and extent of the monitoring which has accompanied this growth. While such monitoring has, by and large, been somewhat limited, the potential for expanded monitoring is clearly present, and warrants careful attention. In particular, I focus here on the issues which have developed around the practice of employee e-mail surveillance, and the ways in which these issues have been framed in the context of public debates. Thus I examine how the issue of employee e-mail monitoring has been presented in the popular media, on the Internet, in political debates, and in statements from various interested parties, including privacy officials and representatives of business and labour organizations. Throughout, my aim is to highlight those aspects of surveillance that have been problematized and by whom, as well as what kinds of solutions have been proposed to address these problems.

E-Mail on the Internet: A Brief History

The emerging importance of e-mail in the workplace reflects the expanding use of electronic networking and of the Internet more generally. Originally a

---

[1] Walter Ulrich, co-founder and board member of the Electronic Messaging Association, as quoted in Jacques Leslie, *Mail Bonding*. Wired 2.03: Electrosphere, pp. 1. Available in electronic form at http://www.hotwired.com/wired/2.03/departments/electrosphere/e-mail.html.
[2] Ibid.

research program of the U.S. Defense Advanced Research Projects Agency (DARPA), the Internetting project was initiated in 1973. The program was designed to investigate techniques and technologies for linking various kinds of networks with the aim of developing "communication protocols which would allow networked computers to communicate transparently across multiple, linked packet networks." [3] The system of networks which emerged from this project is what we know today as the Internet. Its functioning relies on protocols developed as part of that project: the Transmission Control Protocol (TCP) and Internet Protocol (IP), or TCP/IP Protocol Suite.

While the U.S. Federal Government played a pivotal role in supporting the initial development of the Internet, it was joined by other players in the late 1980's as the number of Internet users and network constituents grew. Commercial facilities also began to emerge at that time. Today, "the bulk of the system is made up of private networking facilities in educational and research institutions, businesses and in government organizations across the globe."[4] Plans for government-sponsored research networking continue to be orchestrated by the Coordinating Committee for Intercontinental Networks (CCIRN), which was organized by the U.S. Federal Networking Council (FNC) and the European Réseaux Associées pour la Recherche Européenne (RARE). Their efforts have been key to securing international cooperation in and on the Internet.

The functioning of electronic mail is enabled by the Domain Name System (DNS) maintained by the Internet Registry (IR), which acts as a central repository of Internet information and also allocates network and autonomous system identifiers under the auspices of the Internet Assigned Numbers Authority (IANA): "The Internet Registry (IR) also provides central maintenance of the DNS root database which points to subsidiary distributed DNS servers replicated throughout the Internet. The DNS distributed database is used, *inter alia*, to associate host and network names with their Internet addresses and is critical to the operation of the higher level TCP/IP protocols including electronic mail."[5]

---

[3] Anonymous, *A Brief History of the Internet and Related Networks.* Electronic document, available at gopher://gopher.isoc.org//11/internet/history.

[4] Ibid.

[5] Ibid. I am grateful to Wayne Madsen for alerting me to the politics behind the Internet Registry's allocation of network and system identifiers. In an age of politically contested

In essence, then, e-mail enables users to send written communications between networked computers. Some e-mail systems operate on closed networks, as in the case of in-house networks, but many are connected to the Internet, which allows users to communicate with other users anywhere in the world.[6] Users log on to their host servers, usually by modem, and can then retrieve messages which have collected in their "mailboxes", or send messages out. Normally, the process of logging on requires the user to provide a password. When employers provide their employees with e-mail accounts for business use, a record is usually kept of this password. Even when this is not the case, system administrators are generally able to override or change passwords, though this will often be apparent to the employee next time she attempts to use her account.

It is wholly understandable that e-mail messaging has been seized upon as a business tool with such enthusiasm. The potential benefits of the use of e-mail in business are obvious: electronic mail allows communications to flow easily and efficiently between colleagues and clients, regardless of whether they are across the room or across the world. Evidence suggests that e-mail also "flattens hierarchies, promotes teamwork, and increases involvement of peripheral workers in organizations."[7] These benefits are offered at a time when many companies are facing pressures to increase productivity and incorporate new information technologies.[8] E-mail has been an important aspect of business process redesign, which restructures corporations around information technologies, rather than trying to fit the technology around existing structures.[9] The use of e-mail in the workplace has brought with it the hope of tremendous improvements in efficiency and productivity, and promises to do away with the inconveniences of time and distance.

---

borders and struggles for national identities, the Internet Registry becomes another site where nation-states can achieve, or fail to achieve, international legitimacy through system identifiers.

[6] While messages can be sent between system with relative ease, some of the services associated with particular e-mail systems, such as directories, are lost or significantly complicated by attempts to interface with other systems. On this point, see Nicholas von Hoffman, *The ABC's of E-mail*, Architectural Digest. November 1994, pp. 136.

[7] Leslie, *Mail Bonding*, pp. 1.

[8] Ibid., pp. 2.

[9] The central appeal of business process redesign, which is touted by Michael Hammer and James Champy in their best-selling book, Reengineering the Corporation, is that it eliminates or greatly reduces the need for middle managers, and thereby reduces costs. See Leslie, *Mail Bonding*, pp. 2.

As an added benefit, Internet e-mail can provide access to valuable resources, such as newsgroups and discussion groups, which can be sources of up-to-the-minute information while also serving as informal professional associations.[10]

The tremendous potential afforded by the use of e-mail in the workplace has led some observers to comment that it has "revolutionized the workplace."[11] While this may well be so, the use of e-mail in the workplace has also been the focus of at least two significant and ongoing debates. The first relates to the fact that because e-mail messages travel over the Internet, they are notoriously insecure. This has led some experts to caution that e-mail has about "the same security level as a postcard."[12] This has been an important consideration in the business community, where messages may often contain sensitive or privileged information. In the United States, where there are certain controls on the allowable strength of encryption software for export, heated debates have emerged around issues of network security and e-mail privacy. These debates have been further fueled by the Clinton administration's proposed Clipper scheme, which would build "back doors" into encryption software for access by law enforcement agencies. I return to this debate in a later chapter.

The second debate which has evolved around workplace e-mail has been triggered by the fact that the use of e-mail has been accompanied by an increasing interest on the part of employers in e-mail monitoring. This interest has arguably been fueled by traditional workplace preoccupations, which might arguably include the need to monitor employees and their use of organizational resources, as well as the desire to rationalize work processes as much as possible. Such monitoring can

---

[10] There are some interesting studies on the impact of e-mail in various academic disciplines. These studies suggest that, for example, oceanographers who use e-mail "produce more papers, receive more professional recognition from their peers, and know more physical oceanographers." 1993 study by Sproull, Kiesler, et al. at Carnegie Mellon University, as quoted in Leslie, *Mail Bonding*, pp. 4. Presumably, one would find similar benefits in at least some other fields as well.

[11] Laurie Thomas Lee, "*Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop*," The John Marshall Law Review, Volume 28:137, pp. 140.

[12] Ronald L. Rivest, personal communication reported in Technology Review, August/September 1992, pp. 11, as quoted in Information and Privacy Commissioner/Ontario, Privacy Protection Principles for Electronic Mail Systems, February 1994, pp. 1. A similar statement was made by Marc Rotenberg of EPIC in Charles Piller, *Bosses with X-Ray Eyes*, Macworld, July 1993, pp. 5.

be relatively easily carried out; employees using e-mail leave a sort of electronic trail which can be used to trace the flow of messages, as well as to access the messages themselves. And monitoring can often be carried out surreptitiously since messages remain in the system's memory, backed up on magnetic tapes, even after they have been deleted from the recipient's terminal. This enables system administrators to "monitor the message traffic and store E-mail as a permanent electronic record, and in some cases make and store printed copies."[13] It is the debate which has emerged around this practice, and the concern around the potential for the extension of this practice, which is of interest to me here.

While the monitoring of employee e-mail is, in some sense, simply another form of workplace surveillance, it can be distinguished from other workplace surveillance practices, such as video surveillance, key stroke monitoring, and workplace drug testing, in a number of significant ways. First, e-mail technology is relatively new, and its widespread use in the context of business is even newer. Thus, unlike other forms of surveillance, little has been written on the particular issues that are or might be raised by employee e-mail monitoring. Second, the availability of e-mail in the workplace is linked to participation in various functions of the Internet. The Internet seems to be emerging as an important new forum for social interaction. Thus there are important and timely questions to be asked about what it means that these new sites of social interaction are developing, at least in part, under conditions of surveillance. A third and related difference between e-mail surveillance and other forms of surveillance in the workplace is that self-presentation in e-mail messaging systems is closely linked to questions of identity and community, particularly when e-mail is used to participate in discussion groups and other features on the Internet. The surveillance of e-mail, then, raises significant questions about the effects of surveillance upon the subject, and in particular about whether and how surveillance serves to discipline subjects. These questions are not raised, or are raised only peripherally, by other workplace surveillance practices.

---

[13] Lee, *Watch Your E-Mail*, pp. 141. Lee further notes that "this is what happened in 1990 when the Mayor of Colorado Springs, Colorado, admitted he had been reading the electronic mail that city council members had sent to one another...An E-mail policy had required that messages be printed periodically and be deleted to save space on the city computer." See Don J. Benedictis, *E-Mail Snoops*, A.B.A. J., Sept. 1990, at 26.

Thus a consideration of employee e-mail surveillance provides a particularly good vehicle through which to consider the themes of surveillance and subjectivity.

Employee E-Mail Surveillance: Some Selected Cases

In the past few years, a number of cases involving the monitoring of employee e-mail have focused attention on this practice. These cases have spurred public debate about e-mail privacy while also contributing to debates about workplace surveillance more generally.[14] Perhaps the most famous of these cases was launched in 1992 by Borland International. Borland executives charged that before Eugene Wang, former vice president of computer languages, left to work for Symantec, a direct competitor, he revealed top secret corporate data to Symantec CEO Gordon Eubanks. The corporate secrets, which allegedly included "marketing plans, product release dates, and detailed information of Borland's game plan against Symantec," were transferred to Eubanks using MCI Mail, a commercial electronic mail service that was provided by Borland to its employees.[15]

Wang and Eubanks denied having violated trade secrecy laws and responded to the charges by saying that Borland had violated U.S. federal law by viewing Wang's e-mail messages. Borland countered that it was fully within its rights to inspect Wang's messages since it had provided him with the account. According to a Borland spokesperson, "new employees at Borland are given an MCI [mail] password that is on file with a Borland administrator...You do not have a reasonable expectation of privacy in an E-Mail system that is given to you for company business by your employer."[16]

In a similar case, Alana Shoars, former e-mail director of Epson America, claimed that she was dismissed in March of 1989 for "questioning her boss's rights to read hundreds of e-mail messages sent between other employees."[17] Shoars had been instructed to assure the 700 employees that she trained on the system that

---

[14] Most of the examples and studies cited in this section are American. Unfortunately, there is a real lack of Canadian research on this topic, with a few notable exceptions mentioned below.

[15] Charles Piller, *To Catch a Spy: Is Workplace E-Mail Private*? (sidebar) Macworld, July 1993. pp. 6.

[16] Ibid.

[17] Ibid.

their e-mail messages would be private. She later discovered that her supervisor, who managed the mainframe, had set up a gateway "between Epson's computers and MCI Mail so that he could read all the e-mail from outside the company."[18] Shoars took Epson to court, and a class-action suit was filed on behalf of all the employees whose e-mail had been intercepted.

A third notable case, distinguished from the first two by the fact that it involved an in-house electronic mail system, was brought against the Nissan Motor Corporation. Bonita Burke and Rhonda Hall were fired from their jobs running the e-mail network for Infiniti dealers "after complaining about managers printing and reviewing printouts of personal messages from the company's E-Mail system -- messages they assumed were private."[19] The monitoring began when a supervisor heard that Burke and Hall were receiving personal messages from dealers, including "love letters, soft-core porn and horoscopes."[20] The women were reprimanded and threatened with dismissal. When they filed a grievance for invasion of privacy, Nissan fired them. The two women subsequently sued the company for wrongful termination.

While these cases have been among the most publicized, a 1993 MacWorld survey suggests that they are not isolated incidents.[21] MacWorld surveyed the CEOs and MIS directors of over 300 businesses of various sizes "to see how much they peek at their employees work on their computers, and why."[22] The study represents the conditions experienced by some one million workers and suggests that as many as 20 million Americans may be subject to workplace monitoring. The survey showed that overall, close to 22 per cent of employers have searched the electronic files of their employees, including work files, electronic mail and voice mail messages. In large companies, this figure was closer to 30 per cent. Of the 22 per cent of employers that searched electronic files, over 40 per cent searched e-mail files in particular. Significantly, the survey showed that employees were given advance warning of these searches only one third of the time. The top three reasons for such searches were given as the monitoring of work flow (29.2 per cent),

---

[18] Kathleen Wiegner, *The Trouble with E-mail*, Working Woman. April 1992, pp. 46
[19] "*To Catch a Spy*" pp. 6.
[20] Wiegner, *The Trouble with E-mail*, pp. 46.
[21] For a good introduction to the relevant case law see Lee, *Watch Your E-Mail.*
[22] Piller, *Bosses with X-Ray Eyes*, pp. 4.

and the investigation of thefts (29.2 per cent) and espionage (21.5 per cent). These figures would seem to suggest that the themes of discipline and rationalization are indeed being played out in the context of e-mail monitoring. An earlier study suggested that the top three reasons for auditing the use of intelligent desktop terminals, or electronic workstations, were: 1) to prevent abuse of company computer resources for personal use; 2) to prevent breaches of security and/or confidentiality; and 3) to prevent violations of laws or regulations with respect to the use of client or employee data.[23] Other potential uses of surveillance in the workplace might be "determining the extent of union organizing activity, monitoring activities of workers' reps, and manipulating employees to circumvent their right to engage in protected union activity."[24]

Although the frequency of searches reported by the MacWorld survey was relatively low, with over 70 per cent of the companies that conduct electronic monitoring reporting five or less searches in the last two years, close to 46 per cent of the survey respondents indicated that they consider electronic monitoring to be acceptable, either generally or under some circumstances. It is worth noting that less than 20 per cent of respondents indicated that their company had a policy on electronic privacy. While one could easily make the case that the findings of the MacWorld study are not generalizable, they remain significant both as an example of self-reported behaviour among the organizations surveyed and as an indication of what potential monitoring patterns might look like.

The Evolution of Modern Workplace Surveillance

Although I have argued that employee e-mail surveillance can be distinguished from other forms of workplace surveillance in a number of significant ways, it remains, at one level, but one of the many surveillance practices which have become regular features in the workplace. All such practices, including employee e-mail surveillance as well as key stroke monitoring, video surveillance, and drug

---

[23] United States Congress, Office of Technology Assessment (OTA), The Electronic Supervisor: New Technology, New Tensions. OTA-CIT-333 (Washington, D.C.: U.S. Government Printing Office, September 1987) pp. 103.

[24] K.H. Decker, Employee Privacy Law And Practice. (New York: John Wiley, 1987) pp. 322, as quoted in Michele Jankish, *Monitoring and surveillance in the workplace: Privacy Issues in an international perspective*, Conditions of Work Digest. Volume 12, Number 1, 1993, pp. 17.

testing, arguably have their roots in the historical emergence of the relations of production under capitalism which focus class antagonism and struggle in the workplace.[25] Under these conditions, management emerged as the mechanism through which class relations in the workplace are channeled and ordered. In this context, the managerial imperative has been to exert control over both labourers and labour processes in order to maximize profits. Surveillance has figured prominently in the achievement of these aims and, in many cases, continues to do so.

While managers, in practice, have a variety of different functions, their tasks can be categorized as relating to three primary aims: "1)economic performance, 2) making work productive and workers achieving, and 3) the social impacts and social responsibilities of the enterprise."[26] For my purposes here, it is this second task which is of particular interest, for it is under the guise of efforts to improve productivity that workers have most often found themselves under surveillance. Historically, projects to increase productivity have been principally concerned with the "timing, placing, observing, and checking of work."[27] The notion that surveillance can be used to good effect to increase productivity is a widespread one, and can be traced back to Frederick Taylor's principles of scientific management."[28] Historically,

---

[25] The term "discipline" has a number of senses. I use it here to refer not only to "training that produces obedience, self-control, or a particular skill," (The Oxford Paperback Dictionary. New edition, 1983) but also to suggest linkages with Foucault's reading of discipline as an instance of the functioning of power. For Foucault, discipline defines "how one may have hold over others' bodies, not only so that they may do what one wishes, but so that they may operate as one wishes, with the techniques, the speed, and the efficiency that one determines. Thus discipline produces subjected and practiced bodies, 'docile' bodies." (Michel Foucault, Discipline and Punish: The Birth of the Prison. (New York: Vintage Books, 1979) pp. 138.)

[26] Peter F. Drucker, People and Performance: The Best of Peter Drucker on Management. (New York: Harper's College Press, 1977) pp. 28-31.

[27] Lyon, op. cit., pp. 34.

[28] These principles were summarized in Taylor's paper on "Shop Management" and included: Time study, using the proper implements and methods; functional or divided responsibilities for supervisors; standardization of all tools and implements used in the plant, and also of the acts or movements of workers for each class of work; the desirability of a planning room or department; the use of slide rules and similar timesaving implements; instruction cards for workers. See Benjamin W. Niebel, Motion and Time Study (Eighth Edition). (Illinois: Irwin Publishing, 1988) pp. 13. On the continued relevance of Taylor's principles to modern managerial practices, see, for example, William K. Fallon, ed., AMA Management Handbook(Second Edition). (New York: Amacom, American Management Association, 1983) pp. I-25. It is worth noting that although the idea that surveillance increases productivity is now part of what might be called the popular wisdom of management, especially in North America, numerous sources suggest that this may not always be the case. See, for example,

scientific management has been linked with surveillance in so far as work monitoring has been used to gather information for the initial establishment of schemes of work, and also to ensure that workers conform to set labour processes and meet the production and performance goals determined by management.

Surveillance schemes, then, have been profoundly implicated in attempts to reduce uncertainty about the 'human element' in production. One component of these attempts has been the extension of disciplinary structures well beyond the parameters of the workplace, as employers have become increasingly interested in collecting *personal* information about their employees. The "processing of an ever-increasing amount of information on individual employees [which has] become a perfectly normal element of work life"[29] has been traced to the early practices of the Ford Motor Company, which employed inspectors to gather personal information about its workers. At that time, the information was collected with the intention of

---

Brent Johnson, Technological Surveillance in the Workplace: Monitoring E-Mail, Computer Files, Voice Mail, and Telephone Use Without Crossing the Privacy Line. Electronic Document, available through the Fairfield and Woods Home Page. See also Information and Privacy Commissioner/Ontario, Workplace Privacy: The Need for a Safety-Net. November 1993, pp. 11.

It is worth noting that there has been some substantial movement away from this style of managing workers and worker productivity. Contemporary managers are less likely to foster a culture of mistrust and suspicion in the workplace, and more likely to encourage workers to participate in and feel a sense of ownership toward the corporation's success. On this theme, see, for example, William Bergquist, The Postmodern Organization: Mastering the Art of Irreversible Change. (San Francisco: Jossey-Bass Publishers, 1993). Changes in management philosophy have not, by and large, been reflected in the literature on workplace surveillance, which tends to function from the assumption that the new technologies of surveillance are being applied to traditional management problems. While this may certainly be the case in some contexts, it is misleading to think that changes in management styles do not effect how management goals are achieved, even if the goals of profit and productivity remain fundamentally the same. On this theme, Shoshana Zuboff notes that "[o]bedience has been the axial principle of task execution in the traditional environment of imperative control. The logic of that environment is reproduced when technology is used only to automate. When tasks require intellective effort, however, obedience can be dysfunctional and can impede the exploitation of information. Under such conditions, internal commitment and motivation replace obedience as the primary bond between the individual and the task." See Shoshana Zuboff, *In the Age of the Smart Machine: The Limits of Hierarchy in an Informated Organization*, in Classics of Organization Theory (4th Edition), Jay Shafrtiz and Steven Out, eds. (Florida: Harcourt Brace College Publishers, 1996), pp. 550.

[29] Privacy Protection Study Commission. Personal privacy in an information society: The report of the Privacy Protection Study Commission. (Washington: Government Printing Office, 1977) pp. 223, as quoted in Spiros Simitis, *Developments in the Protection of Workers' Personal Data,* in Conditions of Work Digest: Workers' Privacy, Part 1: Protection of personal data. (Geneva: International Labour Office, 1991) pp. 7.

using it to reconfigure the relationship between workers and machines so that each would fit the other perfectly, thereby ensuring maximum efficiency and productivity. While information was initially collected through informal interviews, eventually a more elaborate system evolved which included elaborate questionnaires and tests which covered "the employees' background, physical and psychological characteristics, abilities, adaptability, commitment, performance and behavior in general."[30] Management would use this information to scrutinize labourers and labour processes and to restructure the production process in order to "eliminate both the origins of malfunctioning and the potential sources of damage."[31]

The belief that systematically collected and continuously updated information about workers is necessary for rational planning and successful monitoring has persisted, in some measure, since these early days of the Ford Motor Company. Of course, methods of collection have become more sophisticated and more specialized; the early information gathering strategies of Ford Motors have been largely replaced by behavioral, human resources, or corporate identity approaches. The principle of data collection, however, has persisted. As a result, the workplace has emerged as an important site of dataveillance.[32]

The collection of personal information about employees has not only become regularized, but has also been considerably broadened in scope since these early days of the Ford Motor Company. In the United States, for example, current and prospective employers increasingly find themselves being required to submit to drug testing as a condition of acquiring or maintaining employment. This practice was legitimated in the 1980's by President Ronald Reagan's national "war on drugs." Even in this country, where public opinion has not yet been whipped up into such a fervor over drugs, the practice of testing employees for drug use is becoming more of an issue. Public attention was focused on this practice in 1994, when the Canadian Civil Liberties Association lodged a complaint against the Toronto

---

[30] Ibid.
[31] Ibid., pp. 8.
[32] Again, the changing nature of work as we near the end of the twentieth century may be slowly eroding the role of the workplace as an information-gathering centre. In particular, the trend toward more contract-style employment and increased job mobility is likely to reconfigure the relationship between workers and employees in ways that impact on the need or ability for workplaces to remain repositories of employee information.

Dominion Bank with the Canadian Human Rights Commission. The Association objected to the Bank's policy of testing all new employees for drug use. While the Human Rights tribunal approved the policy, albeit with some reservations, their decision was overturned in 1996 by the Federal Court of Canada. The Court ruled that the policy was discriminatory, and noted that the Bank had not been able to show any link between drug use and job performance. A similar case involving Imperial Oil in the summer of 1995 served to further heighten public awareness of the issue of drug testing in the workplace.[33]

The expansion of employer-based benefits, such as health care benefits, pensions, and insurance plans has also served to add to the pressure to systematically collect and use personal information about employees. These benefit plans all require the collection and storage of employee information that might not otherwise be available to or required by employers. In some cases, the provision of these benefits takes on a disciplinary function as well. In the United States, for example, companies eager to lower premiums on their employee health insurance packages may prohibit smoking or limit participation in dangerous recreational activities that might result in employees making claims against the company's insurance. In this way, workplace rules are extended so that they dictate behaviour both on and off the job.

The practice of collecting and using personal information about employees, then, has grown under the pressure of the managerial imperative and the expansion of the functions of employers to include the provision of a variety of benefits. In addition to these pressures, governments have come to rely on employers as an important source of information about employees. Thus, for example, governments use information provided by employers as part of the taxation process, and also to administer employee health and safety or training programs. The regulatory interventions of governments into the workplace not only require that employers *disclose* employee information, but also that they *collect* additional information at the outset that might otherwise not have been necessary. This expansion of the employer's role as a collector of information is significant, for it is widely recognized

---

[33] See Canadian Human Rights Commission, Communiqué: Court Rules Drug Testing Policy Discriminatory. Ottawa, April 23, 1996. See also Margot Gibb-Clark, "Drug-test ruling set aside," Globe and Mail (Toronto), April 24, 1996, pp. B1.

that information is susceptible to 'function creep.' In other words, uses are likely to be discovered or devised for information which is already being collected for other, non-work related purposes.[34]

The growth of surveillance in the workplace, then, has historically been a feature of efforts to improve efficiency and productivity while at the same time constituting subjects as particular kinds of workers.[35] As such, surveillance has been one of the most important mechanisms through which power has functioned in the workplace. This, then, is the larger historical and social context within which the monitoring of employee e-mail must be situated. As such, many of the issues raised by the monitoring of employee e-mail are the same ones that have featured in traditional debates about workplace surveillance. Such debates have tended to be heavily focused on the issue of rights and, more specifically, have addressed the problem of defining and weighing the comparative rights of employers and employees with respect to surveillance in the workplace. In such debates, it is always understood that the rights at issue are the right of the employer to monitor productivity, performance, and safety in the workplace and the conflicting right of the employee to enjoy a certain degree of privacy. In such cases, the claim to employee privacy has been a relatively weak protection, for there has been fairly widespread agreement that "our expectation of privacy should not be high during the time that we pursue our livelihoods, and that privacy should be subordinate to other values, principally the collective effort of achieving the goals and objectives of the organization."[36] Nevertheless, the concept of privacy has figured prominently in the anti-surveillance discourse.

---

[34] In Canada, the Social Insurance Number (SIN) is a prime example of this process. Originally, the SIN was created by the federal government as a tool to be used in the administration of taxes. Since each Canadian citizen is issued a unique SIN number, however, the SIN has gained widespread favour as an identification number. In British Columbia, the use of the SIN by public bodies as a means of identification is proscribed by the *Freedom of Information and Protection of Privacy Act*. Private corporations in British Columbia, however, are free to use the SIN with impunity. Thus it is not unusual to be asked for one's SIN when becoming a member at a video store, for example, or applying for a job.

[35] This effect is, perhaps, sometimes unintentional, but other times quite deliberate. See discussion below.

[36] Information and Privacy Commissioner/Ontario, Workplace Privacy: A Consultation Paper. June 1992, foreword.

At the same time, debates around workplace surveillance, and perhaps more specifically *electronic* monitoring, have touched on numerous other issues. Some of these issues related to the "way that electronic monitoring is implemented in a given work environment, some to the use of monitoring to drive the worker, some to the use of information gained in monitoring, and some to the very fact that monitoring is conducted at all."[37] Among the range of specific issues and concerns raised by surveillance in the workplace have been worker participation in job design, worker solidarity and dignity, quality of worklife, and work stress and health.[38]

After privacy, one of the more prominent themes in debates about workplace surveillance has been the issue of consent, and the related theme of worker dignity. Labour groups maintain that, even when employers may have legitimate reasons for monitoring employees, such monitoring should not take place without the prior consent of the employee. Furthermore, they argue that monitoring should not be carried out in ways that suggest that all employees are dishonest or somehow guilty.[39] Business groups, by contrast, argue that employers are fully entitled to determine whether and when monitoring should be undertaken, and that worker consent is not relevant. In a statement to the Information and Privacy Commissioner of Ontario, one such group noted that "privacy rights must be balanced against other valid rights; specifically in this case the rights of employers. One cannot protect privacy rights at the expense of the health and safety of employees or the general public. It is essential that employers have all the information necessary to ensure that proper health and safety practices are being implemented at all times. Health and safety considerations must be paramount."[40] This line of reasoning underlines the fact that the extent to which monitoring is currently occurring is not necessarily as significant as the stance toward such monitoring and its potential extension. For the claim that monitoring is, first and foremost, a way of ensuring health and safety

---

[37] OTA, op. cit., pp. 89.
[38] Ibid.
[39] On this theme, see Information and Privacy Commissioner/Ontario, Workplace Privacy: The Need for a Safety Net. pp. 10-12. In his book on drug testing, John Gilliom argues that the rise of monitoring can be traced to the belief among corporate managers that workers are the cause of all workplace problems, and that they must consequently be subjected to tighter controls. See John Gilliom, Surveillance, Privacy, and the Law: Employee Drug Testing and the Politics of Social Control. (Ann Arbor: The university of Michigan Press, 1994).
[40] Information and Privacy Commissioner/Ontario, op.cit., pp. 14.

in the workplace is, at least partially, a strategic one. First, the MacWorld study indicated that health and safety concerns were not even among the top three reasons for workplace monitoring. Second, there is some evidence that "monitoring increases employee boredom, tension, anxiety, depression, anger, and fatigue."[41] Such conditions are unlikely to contribute to improved health or safety in the workplace. Thus the relationship between surveillance and stress, and also between stress and health, has been a major point of contention in debates around workplace surveillance.

The claim that monitoring is a way to ensure health and safety in the workplace, then, must be understood, in part, as an attempt to manipulate the discourse around workplace surveillance in such a way as to identify employers with the public interest in health and safety while making the claim to privacy rights seem petty or exaggerated. This is not to suggest that employers have no legitimate interests in surveillance whatsoever. Rather, I want to call attention to the kinds of discursive strategies that they have used to express particular interests within the context of public debates about surveillance in the workplace. These strategies have, for example, given rise to public debates about whether privacy is good or bad.[42] Although this approach has enjoyed some measure of success, it has also met with a fair bit of resistance. In Canada and the United States, particularly, people seem to have quite a high expectation of privacy in the workplace, even when that expectation may not be supported by statutory provisions. United States Senator Paul Simon has commented that "[a]s Americans, we feel that our mail is privileged and private, regardless of where or how we receive it."[43]

---

[41] Study conducted by the University of Wisconsin and the Communications Workers of America, as reported in Piller, *Bosses with X-Ray Eyes*, pp. 6. The study confirmed the findings of earlier studies that identify monitoring as a major contributor to workplace stress and feelings of powerlessness.

[42] Stephen Levy, *The Encryption Wars: Is Privacy Good or Bad?* Newsweek, April 24, 1995. pp. 55+.

[43] Bronwyn Fryer and Roberta Furger, *Who's Reading Your E-mail?* PC World. August, 1993. pp. 171. Bill Gates of Microsoft concurs, adding that "people expect exactly the same thing from e-mail that they expect from voice mail or from a conversation -- that is, no bugging." *op. cit.*

Employee E-Mail Surveillance: Emerging Issues in the Postmodern Workplace

While the concerns which have characterized larger debates about workplace surveillance are clearly relevant to debates about the monitoring of employee e-mail more specifically, e-mail raises a variety of issues which are not featured in these larger debates. These specific concerns derive not only from the fact that e-mail is an *electronic* form of surveillance, but also from e-mail's unique status as a relatively new communicative form. Thus, for example, one finds that concerns about the surveillance potential of electronic technologies are clearly and consistently articulated in debates over e-mail privacy. Reports of the monitoring of electronic mail messages seem to feed into a growing anxiety that technology is being used as an instrument of social control and that it may be having social effects that were unanticipated and/or undesirable.[44] As at least one observer has noted, automatic surveillance is often just a useful by-product of electronic systems, and not their raison-d'être.[45] Consequently, too little attention has been paid to the effects of that surveillance. Debates about the monitoring of employee e-mail, then, are clearly invested in larger debates about how the relationship between technology and society is or should be ordered.

The monitoring of employee e-mail also brings to the forefront questions about the extent to which individuals retain a right of privacy in the workplace. When employers argue that they are entitled to monitor e-mail messages, they do so based on the understanding that anything that happens on company time, using

---

[44] On this theme, see John Whalen, *You're Not Paranoid: They Really Are Watching You*, Wired. March 1995, pp. 76+; Langdon Winner, *Who will we be in cyberspace?* The Network Observer. Volume 2, Number 9, September 1995; Victoria A. White, *Ethical Implications of Privacy in Electronic Mail*, from Proceedings of Technical Conference on Telecommunications R&D in Massachusetts, University of Massachusetts Lowell, October 25, 1994. Much has been written on the theme of the place of technology in society more generally. See, for example, Langdon Winner, Autonomous Technology. (Cambridge, Massachusetts: MIT Press, 1992); Jacques Ellul, The Technological Society. (New York: Vintage Books, 1964); Ursula Franklin, The Real World of Technology. (Ontario: Anansi Press, 1992); Siegfried Giedion, Mechanization Takes Command. (New York: W.W. Norton & Co., 1969); Arnold Pacey, The Culture of Technology. (Oxford: Blackwell, 1983); Langdon Winner, The Whale and the Reactor: A Search for Limits in an Age of High Technology. (Chicago: University of Chicago Press, 1986); E.F. Schumacher, Small is Beautiful; Economics as if People Mattered. (New York: Harper & Row, 1973).

[45] Jolyon Jenkins, *Eye Can See You*. New Statesman and Society. 21 February 1992, pp. 14.

company resources, is the property of the company. Thus e-mail accounts which are provided by the company for business purposes are subject to monitoring at the prerogative of the employer. Privacy advocates, however, argue that there is a reasonable expectation of some measure of privacy, even in the workplace. People are generally able to assume that their mail is private, and the same should hold true of *electronic* mail. Furthermore, they note that many workplaces already recognize the rights of employees to maintain some level of privacy in the workplace. This recognition is apparent, for example, in the understanding that employees will sometimes use the telephone for personal reasons, or that they may receive mail of a personal nature at work. If clearly marked, such mail is not normally opened, even in workplaces where most mail is routinely opened before distribution. The same, they argue, should be true of personal e-mail.[46]

A problem which has perhaps served to further cloud the issues has been one of definition. E-mail is a relatively new communicative form, and an ambiguous one at that. For, while "e-mail is written, ...its language typically embodies a shift toward oral speech patterns. It is the most ephemeral of written mediums, lacking the material form of books or letters and capable of being erased in a single keystroke, yet it can be archived and retrieved with unprecedented ease."[47] In some ways, then, e-mail is a sort of hybrid form, falling somewhere between spoken and written communications.[48] As such, the use of e-mail has engendered new forms, as well as new avenues, of social interaction. These emerging forms may well require new policies and norms to govern their use.

---

[46] See Fryer and Furger, *Who's Reading Your E-mail?*, pp. 171.

[47] Leslie, *Mail Bonding*, pp. 1.

[48] I do not want to make too much of the difference between writing and speaking here. The difference is a blurry one at best, and has certainly been the subject of some debate. In his own move from writing to speech, for example, Derrida attempts to "see writing as always already anterior to speech even as it may "follow" speech in a given situation; it is method of interpretation that moves from a search for metaphysically fixed meanings to an exploration of the ambivalent play of differences in the "text"." [Mark Poster, The Mode of Information. (Cambridge: Polity Press, 1990), pp. 102.] So writing, in Derrida's terms, is not "in opposition to speech but anterior to the distinction between speech and writing." [Poster, pp. 102.] Of course, Derrida is not alone in his consideration of the relationship between writing and language. Anthony Giddens and others have also contemplated this relationship. See Anthony Giddens, Social Theory and Modern Sociology. (Cambridge: Polity Press, 1987), especially pp. 100. My casual differentiation between speech and writing above is not at all intended to forestall the kinds of detailed analyses that Derrida and Giddens advance.

Furthermore, some observers have commented that the use of e-mail in the workplace greatly facilitates open communication along non-hierarchical lines. With e-mail, the normal flows of communication up the chain of command can be easily circumvented. This has led some commentators to speculate that the use of e-mail in the workplace has a democratizing effect.[49] While some evidence would seem to suggest that these effects have been somewhat exaggerated,[50] the use of e-mail in the workplace, as elsewhere, clearly does have the potential to alter communication flows in significant ways.[51]

While e-mail has certainly been beneficial in opening up channels of communication, the novelty of the medium has required some negotiation. Because e-mail straddles the traditional divide between written and spoken communication, it does not conform, or conforms only very loosely, to accepted patterns of expression and interpretation in written communication. The development of "netiquette" -- a sort of informal code which attempts to establish shared meanings between e-mail users in order to facilitate communication and forestall misunderstandings -- has been a partial response to problems of expression and interpretation in this new medium.[52] "With e-mail there is no official memo form, no body language or tone of voice to indicate whether a comment is in jest or for real."[53] Netiquette, then, provides a set of interpretive guidelines. Thus, for example, a message written in uppercase is generally understood to be the equivalent of shouting in spoken communications. Similarly, messages written entirely in lower case indicate that the writer is mumbling or rambling.[54] In addition, a variety of symbols have been

---

[49] Leslie, *Mail Bonding*, pp. 1.
[50] Ibid., pp. 3.
[51] Ibid. See also Kantrowitz et al, pp. 71.
[52] Netiquette has not, however, been able to address issues of gender on the Internet. For an overview of how gender is expressed in communicative styles on newsgroups, see Susan Herring, *Gender Differences in Computer-Mediated Communication: Bringing Familiar Baggage to the New Frontier*. Electronic document, available at gopher://gopher.cpsr.org:70/ /00/cpsr/gender/herring.txt.
[53] Kantrowitz et al., pp. 71.
[54] There are a variety of sites which relate to netiquette, many of which contain some kind of list of acceptable standards of behaviour. Elements of these lists have been reproduced in a variety of places. For a good general overview, see the Netiquette Home Page at http://rs6000.adm.fau.edu/rinaldi/netiquette.html, or the (other) Netiquette Home Page at http://bookfair.com/Services/Albion/nqhome.html. Topics covered include rules for one-on-one interaction, the use of symbols for emphasis, smileys, emotional messages, and chain letters.

developed which mimic facial expressions, helping to further clarify both meaning and tone.[55]

As a new form (and forum) of social interaction, e-mail has also raised some interesting questions about identity and community. The Internet address that each e-mail user is assigned provides access to what might loosely be called "electronic communities." One's identity in such communities is "defined by their electronic mail address.[[56]] This transient assemblage of letters and digits provides a non-physical basis of identity. The virtual self may act as a proxy of the physical being holding a similar name, or it may not. This metaphysical puzzle is created by the technology and networks employed to gain access to this community."[57] So while the virtual self is, in some sense, defined by one's e-mail address, this definition is by no means a necessarily stable or unambiguous one. In MUDs, MOOs, and newsgroups, in particular, e-mail and similar forms of electronic communications provide a vehicle for rethinking and repackaging one's identity. In this way the net encourages, or at least allows, a certain degree of playfulness in the presentation of the self. As such,

---

[55] Netiquette also arguably provides for disciplinary measures to be taken against those who break its rules in the form of "flaming." Flame has been defined as: "1. To post an e-mail message intended to insult and provoke. 2. To speak incessantly and/or rabidly on some relatively uninteresting subject or with a patently ridiculous attitude. 3. Either of senses 1 or 2, directed with hostility at a particular person or people." Taken from *Flame*, unattributed electronic document, available at http://nws.cc.emory.edu/Jargon30/JARGON_F/FLAME.HTML. The word is used most often in this third sense. For an interesting discussion of gender differences in flaming, see Herring, *Gender Differences in Computer-Mediated Communication* and also *Politeness in Computer Culture: Why women thank and men flame*, in Communicating Across Cultures: Proceedings of the Third Berkeley Women and Language Conference. Bucholtz and Sutton, eds. Berkeley Women and Language Group. On flaming more generally, see, for example, John Seabrook, *My first flame*. The New Yorker, June 6, 1994, pp. 70-79.

[56] It is possible to shield one's identity on the Net using an anonymous remailer. Using the Coalition for Computer Ethics' "Ten Commandments of Computer Ethics" as a basis, however, White suggests that it is unethical for users to filter messages through anonymous remailers unless there is fear of recrimination for telling the truth. White's argument is not particularly convincing, but it does highlight the fact that there is some controversy about the use of anonymous remailers. See *Ethical Implications of Privacy in Electronic Mail.* Cypherpunks and crypto rebels, of course, take quite the opposite view, arguing that anonymous remailers are a vital weapon in the fight to preserve privacy and anonymity in networked environments. The lack of agreement concerning the proper place of anonymous remailers in electronic communities reflects larger debates about the weight of privacy in relation to other rights and/or interests. This debate is explored in chapter three of this thesis.

[57] White, op. cit.

it breaks significantly with other forms of communication where the stability of the subject is essential to the coherence of the interaction.

The ambiguity of the subject in e-mail exchanges is further exacerbated by the fact that, although it is common to speak in terms of e-mail *addresses*, the assemblage of letters and numbers that makes up those addresses is more accurately represented as an *access code*. This access code is associated with storage space on a computer located somewhere along the network. A user can connect to that storage space from anywhere and retrieve the contents of her in-box or empty her out-box. But regardless of where the person is at that time, his or her e-mail address does not change. An e-mail address, then, cannot tell you where a person was when they sent you a particular message; they may have been connected directly to the mainframe at work or on campus, for example, or they may have been at home, or at a pay phone halfway across the world. In this sense, an Internet access code (or e-mail address) is as much a name as it is an address -- "[t]he categories are conflated due to the simultaneous redefinitions of space, personal identity, and subjectivity that are emerging as the network grows."[58]

If the identity and location of the e-mail user are ambiguous and unstable, these ambiguities are clearly reflected in so-called electronic communities. Such communities have no geographical basis, but rather represent groupings of people with similar interests, opinions, or concerns.[59] These communities are, in a very real sense, chosen rather than assigned by accidents of birth or proximity.[60] Because the net comprises so many of these communities, it is somewhat misleading, though common in the popular media, to refer to the electronic community in the singular. Instead, it is more accurately conceived of as a complex tapestry of many different communities, some linked and some isolated.

The coexistence of so many virtual communities leads one to consider the effects of the network on civic culture. Winner notes that "to invent a new technology requires society to invent the kinds of people who will use it, with new

---

[58] City of Bits WWW Team, *Electronic Agoras: Spatial/Antispatial*, from the City of Bits Web Page: http://www-mitpress.mit.edu/city_of_bits/welcome.html.

[59] The fact that there is very little commonality among electronic communities is reflected in the lack of shared values on the net. On this theme, see White, op. cit.

[60] On this theme, see J.C.R. Linklider, et al, *The Computer as a Communication Device*, International Science and Technology. April 1968, pp. 1.

practices, relationships, and identities supplanting the old."[61] Thus, he argues, it is important to interrogate new technologies and new systems with the following questions:

1. Around these instruments, what kinds of bonds, attachments and obligations are in the making?
2. To whom or to what are people connected or dependent upon?
3. Do ordinary people see themselves as having a crucial role in what is taking shape?
4. Do people see themselves as competent to make decisions?
5. Do they feel that their voices matter in making decisions that will affect family, workplace, community, nation?[62]

While Winner's concern is not with electronic mail technologies in particular, his questions bear keeping in mind in the context of the spread of these technologies in the workplace.

The monitoring of e-mail accounts provided to employees for business use, then, clearly raises a number of important issues, some of which I have touched on here. The framing of the problem of e-mail monitoring in public debates, however, has tended to highlight only a few of these issues. In particular, public discussion has been centrally preoccupied with the theme of rights. The rights that are taken to be at issue here, as outlined above, are the right of the employer to monitor labour and labour processes to ensure maximum productivity and profitability, and the competing right of employees to enjoy a certain degree of privacy and dignity while they are on the job.

This particular framing of the issue has tended to favour the employer, particularly since it seems to be generally agreed that employees lose their claim to a right of privacy when their employers develop and disseminate policies which explicitly warn them that their messages may be subject to surveillance.[63] This would seem to imply that it is not so much *privacy* as *consent* (in a very loose sense of the word) which is at issue here. Furthermore, most newspaper and popular magazine articles which address this theme suggest that, in the absence of such

---

[61] Winner, *Who Will We Be in Cyberspace*?, pp. 1.
[62] Ibid., pp. 1-2.
[63] See, for example, Fryer and Furger, *Who's Reading Your E-mail*? and Piller, *Bosses with X-Ray Eyes*. Based on this idea, the Electronic Mail Association publishes an E-mail policy handbook which tells employers how to develop e-mail policies appropriate to their specific circumstances. See also Brent T. Johnson, op. cit.

policies, employees should assume that their mail is being or may be read.[64] The validity of employees' claim to a right of privacy, then, appears to be largely up to the discretion of the employer. In this sense, it is perhaps misleading to refer to privacy as a *right*, rather than, say, a value or a good.

Still, privacy has continued to be the rallying point for moves to limit or eliminate employee e-mail surveillance. In Ontario, the Information and Privacy Commissioner's Office developed a list of principles for the use of electronic mail systems. These principles highlight the centrality of privacy in the anti-surveillance discourse. The principles are listed as follows:

1. The privacy of e-mail users should be respected and protected.
2. Each organization should create an explicit policy which addresses the privacy of e-mail users.
3. Each organization should make its e-mail policy known to users and inform users of their rights and obligations in regard to the confidentiality of messages on the system.
4. Users should receive proper training in regard to e-mail and the security/privacy issues surrounding its use.
5. E-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy.
6. Providers of e-mail systems should explore technical means to protect privacy.
7. Organizations should develop appropriate security procedures to protect e-mail messages.[65]

Characteristically, neither these principles nor the report in which they appear addresses the underlying question of how far the entitlement to privacy in the workplace extends.[66] Furthermore, they are arguably somewhat benign, since their

---

[64] See, for example, Barbara Kantrowitz and Betsy McKay, *Who Holds the Key to the E-mailbox*? Newsweek. 12/20/93, Volume 122, Issue 25; David Bjerklie, *E-Mail: The Boss is Watching*. Technology Review. April 1993, Volume 96, Issue 3; Keith Hammonds et al, *E-mail: Beware of Big Brother*. Business Week. 3/4/96, Issue 3465; *Employee E-Mail: Is it Really Private*? Nation's Business. March 1996, Volume 84, Issue 3; W.D. Riley, *Mine! Mine! Mine!* Datamation. 9/1/95, Volume 41, Issue 16; K.P., *E-Mail Keeps No Secrets*, Canadian Living. December 1994, Volume 19, Issue 12; Philip Elmer-Dewitt et al., *Who's Reading Your Screen?* Time. 1/18/93, Volume 141, Issue 3; K. Wiegner, *The Trouble With E-Mail*, Working Woman. April 1992, Volume 17, Issue 4; Robert Fulford, *Tolerating Electronic Sweatshops*, Globe and Mail. December 14, 1994, pp. A12.

[65] Information and Privacy Commissioner/Ontario, Privacy Protection Principles for Electronic Mail Systems., pp. ii.

[66] British Columbia's Information and Privacy Commissioner has also confronted the issue of e-mail, albeit in a somewhat different context. See Office of the Information and Privacy Commissioner for the Province of British Columbia, Order No. 121-1996: INQUIRY RE: A

main emphasis is on the need for *policies* concerning privacy of e-mail, rather than on the need for *privacy* in e-mail. Thus, once again, these principles contribute to an understanding of the problem as one of consent or notification, rather than one of privacy per se.

While the kinds of principles which are listed above have generally been supported by privacy advocates, the claim to a right of privacy in the workplace has afforded relatively weak protection against the mounting tide of surveillance. Certainly, it has not been enough to stop the growing interest in e-mail monitoring among employers.[67] One must ask, then, why it is that the claim to privacy has provided such weak protection against e-mail monitoring, and against workplace surveillance more generally. The quick response is perhaps that employee privacy has only a limited place in the workplace. But this response seems insufficient, for it does not address the underlying question of why that should be the case. Furthermore, even in offices where all incoming mail is opened and logged before being distributed, envelopes marked "personal and confidential" are usually passed along to the recipient unopened. Some measure of privacy is clearly being respected here, and it seems odd that this courtesy should not be extended to electronic mail messages as well.

What is it about the employer's claim to a right to monitor, then, that seems to defeat the claim to a right of privacy so definitively? There are many possible answers to this question, but I would argue that perhaps the most persuasive of these is that the employer's claim to a right to monitor taps into what might be called the "will to efficiency." North American culture has been obsessed with efficiency, and has embraced the idea that "because something efficient can be done, it must be done."[68] As one of the tools in the management arsenal, workplace surveillance

---

decision by the Ministry of Agriculture, Fisheries and Food to refuse access to computer backup tapes containing deleted e-mail. September 3, 1996. Available in electronic form at http://latte.cafe.net/gvc/foi/orders/Order121.html.

[67] Toronto news stations reporting on COMDEX Canada '96, an international computer trade show which was held in Toronto from July 10 to 12, 1996, indicated that the most popular and the most talked-about exhibitors were those showcasing software that enabled the monitoring of electronic workstations.

[68] Fulford, *Tolerating Electronic Sweatshops*, pp. A12. Of course, there have been a number of very influential commentators on the theme of efficiency as a feature of modern social organization. See, for example, Winner, op. cit.; Ellul, op. cit.; Franklin, op. cit.; Giedion, op. cit.; Pacey, op. cit.; Winner, The Whale and the Reactor op. cit., Schumacher, op. cit., and

has been closely linked to projects to improve efficiency and to rationalize labour processes in the name of improving profitability. As a result, surveillance in the workplace has gained significant legitimacy, even if it does not always actually improve efficiency or achieves these improvements at a tremendous human cost.

It is this cultural fascination with efficiency, I would argue, that has rendered privacy such a weak protection against the claims of employers with regards to workplace monitoring. This weakness has been further exacerbated by the tenuity of the claim to a "right" of privacy in the workplace, which seems, in many cases, to rely upon the goodwill of the employer. By and large, the onus has been on employees and privacy advocates to show why the employer's right to monitor should not predominate. Consequently, employers have been in a relatively good position with respect to public debates about employee e-mail monitoring. While they may not have been successful in swinging the tide of public sympathy in their favour, their claims seem irrefutable, or at least strongly compelling, within the present parameters of the debate.

In the next chapter, then, I consider the larger terrain within which the present debate has been contained. More specifically, I situate the debates around employee e-mail monitoring within larger discourses of surveillance in order to come to some understanding of why the debate around employee e-mail monitoring has unfolded in the way that it has. Focusing on the growth of the modern military, bureaucracy, and capitalism as stimulants to surveillance, I identify surveillance as an important feature of modernity. I do so in order to demonstrate the need to consider the development of modernity, and the relationship between surveillance and modernity, in building any meaningful understanding of contemporary surveillance practices. Such consideration is generally not evident in either the public or the academic discourses around surveillance, and this lack is reflected in how the issue of surveillance has been problematized within those discourses.

Max Weber, *The Meaning of Discipline* and *Bureaucracy*, From Max Weber: Essays in Sociology. H.H. Gerth and C. Wright Mills, eds. (New York: Oxford University Press, 1958).

Chapter Two: Situating Workplace Surveillance

In order to understand how debates about employee e-mail monitoring have come to be framed in particular ways, it is useful to consider the broader social context in which such debates have occurred. As I outlined in the previous chapter, the monitoring of employee e-mail fits into larger and well-established patterns of workplace surveillance. These patterns, in turn, both participate in and reflect the widespread extension of surveillance which has characterized modern societies. Modern societies have been so invested in the production and consumption of information as a commodity that some commentators have suggested that we are now, or soon will be, living in what they call "surveillance societies."[1] The roots of such societies are to be found not in a single historic moment, or in the evolution of any particular set of surveillance practices, but rather in the complex interplay of a number of factors over an extended period of time. In general terms, these factors are also implicated in the growth of modernity, and in the growth of specifically modern forms of the state, the military, industrialization, urbanization, government administration, and the capitalist business enterprise.[2] This has led David Lyon, for example, to argue that modern societies are and always have been "information societies."[3] He suggests that the decisive factor in the development of these societies is the growth of democracy, and the "post-Enlightenment political demand for equality" that displaced or diluted older forms of surveillance which were enacted at the local, familial, and religious levels.[4] As these traditional sites of surveillance went into decline, emerging nation-states and the burgeoning machinery of capital took over their surveillance functions.

It is clearly beyond the scope of this project to provide a detailed account of the emergence of modernity.[5] In this chapter, then, I focus on those aspects of modernity

---

[1] See, for example, Flaherty, Protecting Privacy in Surveillance Societies, Marx, Undercover, and Davies, Big Brother.

[2] Lyon, op. cit., pp. 24.

[3] On this point, see also James Beniger, The Control Revolution: Technological and Economic Origins of the Information Society. (Cambridge Massachusetts and London, England: Harvard University Press, 1986).

[4] Ibid.

[5] There is a fairly substantial and growing literature on this theme. Some good sources would include the following: Anthony Giddens, The Consequences of Modernity (Cambridge, UK: Polity

which have been most invested in the development of surveillance as a feature of the workplace, either as a strategy of discipline or, more generally, as an expression of power. Although one could make the case that all aspects of modernity are invested in surveillance as a disciplinary strategy generally,[6] my focus here is on the growth of the military, the evolution of the bureaucratic form, and the development of management as a technology of surveillance within the context of the capitalist business enterprise.[7] My decision to limit myself to these aspects of modernity reflects my belief that the military, bureaucracy, and capitalism have been among the most important influences on the development of surveillance practices in the specific context of the workplace. The literature on surveillance, however, has, by and large, failed to consider these influences seriously. This failure has had important implications in terms of limiting the kinds of analyses that are provided by that literature. I want to use this chapter, then, to address some of those limitations.

The reader will notice, no doubt, that there is very little discussion here of the role that technology has played in enabling or stimulating certain forms of surveillance, either in the workplace or elsewhere. This omission is quite deliberate; the literature on surveillance has tended to place a heavy emphasis on technology as a contributing factor to surveillance. This emphasis, I would argue, has had the effect of diverting

---

Press, 1990); Christopher Dandeker, Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day. (New York: St. Martin's Press, 1990); Daniel Bell, The Coming of Post-Industrial Society. (New York: Basic Books, 1973); Richard J. Bernstein, The New Constellation: The Ethical-Political Horizons of Modernity/Postmodernity. (Cambridge, UK: Polity Press, 1991); Zygmunt Bauman, Intimations of Postmodernity. (London and New York: Routledge, 1993); Arthur Kroeker, The Possessed Individual: Technology and Postmodernity. (London: Macmillan, 1992); Bryan S. Turner, ed., Theories of Modernity and Postmodernity. (London and California: Sage Publications, 1990); Joyce Appleby, Knowledge and Postmodernism in Historical Perspective. (New York: Routledge, 1996). Excellent analyses of the emergence of the conditions of modernity can also be found in feminist and post-colonial literatures.

[6] This theme appears in a number of Giddens' works, most notably in The Nation State and Violence (Cambridge, UK: Polity Press, 1985) and The Consequences of Modernity (op. cit.).

[7] One of several very interesting areas which I do not touch on here is the role of surveillance, broadly defined, in maintaining gendered identities within power structures which are characterized as patriarchal or hetero-patriarchal. Marilyn Frye's work on this theme is insightful. Frye argues that gender is produced and reproduced, in part, under the surveillance of the "arrogant [masculine] eye" which watches for and punishes transgression. This have been a recurrent theme in feminist and queer theory. See Marilyn Frye, The Politics of Reality: Essays in Feminist Theory. (Freedom, California: The Crossing Press, 1983). See also Judith Butler, *Imitation and Gender Insubordination*, Inside/Out Diana Fuss, ed. (New York and London: Routledge, 1991).

attention away from other factors which have been at least equally relevant to the development of contemporary surveillance practices. Indeed, one of the principal points of this chapter is that the focus on technology in the surveillance literature has tended to obscure the ways in which larger and more generalized historical patterns, including the growth of the military, the bureaucracy, and management techniques, have provided the necessary conditions for the appearance of certain technologically-enhanced surveillance structures.

Thus, for example, I would argue that is not simply because new technologies exist that it makes sense to talk about a "new surveillance." Such facile distinctions miss the point about whether contemporary forms of surveillance constitute subjects differently than did more traditional forms. The failure to consider these kinds of questions renders distinctions between new and old forms of surveillance largely irrelevant, for there is little force in the claim of a new surveillance if the experience and the effects of surveillance have not changed? This is not to suggest that this chapter is devoted to whether or not there is a new surveillance. Rather, I want to argue that the criteria by which we determine whether surveillance is new or not must be more comprehensive and that, in particular, it must take into account the ways in which contemporary patterns of surveillance reflect the development of certain aspects of modernity. These aspects include, but are not limited to, the growth of the military, the evolution of the bureaucratic form, and the development of surveillance as an aspect of management techniques. An understanding of these aspects provides a clearer understanding of the social context in which surveillance has emerged and is emerging, while at the same time providing a theoretical framework within which to consider what the social effects (intended or otherwise) of surveillance are and have been. Such an understanding might do much to forestall grandiose claims about "information societies" which are based on an analysis of new technologies alone, and do not consider sociology, economics, or politics.[8]

In my treatment of the growth of the military, bureaucracy, and capitalism, I am principally concerned with the themes of discipline and rationalization, and the ways in

---

[8] Such claims are made, for example, by Don Tapscott (see The Digital Economy: Promise and Peril in the Age of Networked Intelligence. (New York: McGraw Hill, 1996) and Paradigm Shift: The New Promise of Information Technology. (New York: McGraw Hill, 1992)) and also by Nicholas Negropante of MIT's MediaLab.

which these themes have been played out in these particular contexts. These themes are occasionally touched upon in the literature on surveillance, but usually in very superficial ways. In that literature, only the sociologists have really taken seriously the relationship between surveillance and social control. So I begin my analysis here by considering how the rationalization of the armed forces led to a demand for greater discipline within the ranks. This demand was met, in part, by the development of surveillance structures within the military which were then extended, though only in part, to civilian society. A similar process of rationalization is reflected in the emergence of the bureaucratic form of organization with its emphasis on record-keeping and efficiency. Through bureaucracy, the necessary preconditions for a regime of dataveillance are achieved, and the exchange of information for rights and services is regularized and normalized. The extension and adaptation of bureaucratic techniques of organization into the capitalist workplace in the form of management contributes further to regimes of dataveillance, while at the same time introducing new forms of surveillance which make it possible to collect specific and detailed information about the activities of an employee inside and outside the workplace. A number of forces operating both inside and outside the workplace combined over time to extend the collection of information to consumers, and a new era of targeted marketing was ushered in.[9]

That literature which *has* concerned itself with theorizing the emergence of contemporary surveillance societies has been primarily sociological in origin. This is not surprising given that the sociological literature on surveillance has been concerned with the problem of understanding the relationship between contemporary surveillance practices and social order. Analyses of the emergence of surveillance societies provide a context for thinking about that relationship. In working through the relationship between surveillance and society, the sociologists have been greatly influenced by Max Weber, Karl Marx, and Michel Foucault. That influence has been apparent not only in shaping the major preoccupations of that literature, but also in the framing of its various problematics.

---

[9] For a detailed discussion of these forces, see Oscar Gandy Jr., The Panoptic Sort: A Political Economy of Personal Information. (Colorado: Westview Press, 1993). See also Lyon, op. cit.

Disciplined Statehood: The Growth of the Modern Military

Perhaps the most significant theme to have preoccupied the literature on the emergence of surveillance societies has been the relationship between surveillance and discipline. An obvious starting point for understanding this relationship is the military. In his essay on *The Meaning of Discipline*, Max Weber argued that "the discipline of the army gives birth to all discipline."[10] The armed forces have certainly had a place of honour in the history of the growth of surveillance, and of modernity more generally, for they were the site of the early modernization efforts which would eventually serve as a blueprint for other organizational forms. The broad influence of modernization projects in the armed forces reflect their central role in the creation of the early modern state. Lyon notes that "warfare with other societies helped create the modern state as an entity separate from civil society and with the organizational means of supervising the population of a given territory."[11] As a result, the military has enjoyed, and continues to enjoy, a certain privilege within modern nation states.

The privileging of the military has contributed to the growth of state-generated surveillance in a number of ways. First, states of war have generally enabled the extension of state supervision into the lives of citizens. During the First and Second World Wars in particular, whole societies became involved in the process of warfare through 'war efforts.' As a result, "public opinion had to be monitored in new ways, and production and distribution regulated as never before, to ensure that in conditions of total war victory was achievable."[12] Second, the protection of citizens against external threats has tended to involve the suspension or erosion of certain civil liberties, including the right of assembly and the right of mobility. In practice, the suspension of these liberties often includes a surveillance component such as the required use of identity cards, for example. Finally, the military has developed a wide variety of surveillance technologies, some of which have subsequently been put to use by other organizations, such as law enforcement technologies. In this way, sophisticated surveillance techniques have become more widely available and more widely used.

---

[10] Max Weber, *The Meaning of Discipline*, From Max Weber: Essays in Sociology. H.H. Gerth and C. Wright Mills, eds. (New York: Oxford University Press, 1958) pp. 261.
[11] Lyon, op. cit., pp. 28.
[12] Ibid., pp. 29

Historically, modernization has also been an important part of the role of the military in extending state surveillance. Early modernization in the military can be traced at least as far back as the leadership of Maurice of Nassau, Captain-General of Holland and Zeeland from 1585 to 1625. Maurice built upon the Roman idea of the systematic drill by dividing his army into small tactical units. "Soldiers were taught to regularize their marching, as [sic] to load and fire their matchlock guns in the forty-two moves analyzed by Maurice, thus permitting constant volleys of fire."[13] These drills were supervised by a new cadre of officers which insure maximum efficiency and peak performance. In this way, the modern army was born, "complete with an embryonic bureaucracy, a separate class of officials or officers, uniforms, and disciplined drill, all in the quest for efficiency and the need to reduce unit costs."[14] Thus Maurice's rationalized military organization is not only the foundation of the modern armed forces, but also an important point in the emergence of supervisory techniques.

While Maurice's army represents what was perhaps the first concerted effort at rationalizing the armed forces, the military was engaged in the project of discipline long before Maurice's time. Max Weber traces the disciplinary patterns of the modern army to the Hellenic and Roman Hoplites, who were prohibited from fighting out of line.[15] Weber also reads the history of weaponry as a history of discipline, arguing that "the kind of weapon has been the result and not the cause of discipline."[16] Thus, for Weber, gun powder and the technologies of war that are associated with it only became significant as a result of the success of formalized disciplinary structures.

It was not until Maurice's time, however, that the content of discipline became solidified as the "consistently rationalized, methodically trained and exact execution of the received order, in which all personal criticism is unconditionally suspended and the actor is unswervingly and exclusively set for carrying out the command."[17] Under these conditions, conduct could be ordered in such a way as to be rationally uniform and therefore predictable. As a result, it became possible, at least in theory, to calculate the "optimum of physical and psychic power in attack."[18]

---

[13] Ibid., pp. 27.
[14] Ibid.
[15] Weber, *The Meaning of Discipline*. pp. 256. The Hoplites were heavily armed foot-soldiers.
[16] Ibid.
[17] Ibid., pp. 253.
[18] Ibid., pp. 254.

At the same time, discipline in the modernized military developed a distinctly impersonal character, which is to say that it was no longer necessarily associated with the charisma of a leader or group of leaders. Instead, a sense of duty which was identified with a 'cause' in the broadest sense was cultivated. Weber argues that such a shift was inevitable, for it is "the fate of charisma, whenever it comes into the permanent institutions of a community, to give way to powers of tradition or of rational socialization."[19] Weber identified the waning of charisma as a sign of the diminishing importance of individual action in the context of rational discipline, which requires a group dynamic of rationally uniform obedience.

For Weber, the sociologically decisive features of modernized military discipline are

> first, that everything, and especially these 'imponderable' and irrational emotional factors, are rationally calculated -- in principle, at least, in the same manner as one calculates the yields of coal and iron deposits. Secondly, devotion, in its purposefulness and according to its normal content, is of an objective character. It is devotion to a common 'cause,' to a rationally intended 'success'; it does not mean devotion to a person as such -- however 'personally' tinged it may be in the concrete instance of a fascinating leader.[20]

The modernization of military discipline has served as a blueprint for similar projects in other organizational settings. As a result, the sociological features that Weber identifies as being characteristic of the modern military reappear in a variety of contexts, including government administration, industrial organization, prisons, and educational institutions. In each case, as in the military, the maintenance of disciplinary structures has operated, in part, through a system of rules which construct and constrict both behaviour and analysis. These rules operate to force human behaviour to approach, if not to achieve, rational uniformity in order to facilitate rational decision-making. So rationalization projects have clearly been heavily invested in creating the conditions under which obedience becomes not only possible, but virtually inescapable.

---

[19] Ibid., pp. 253.
[20] Ibid., pp. 254.

Everyday Surveillance: Bureaucracy and the Modern State

Bureaucracy is one organizational technique through which the state, using the mechanisms of government, has created the conditions necessary to insure obedience. Indeed, Weber argues that bureaucracy is the most rational offspring of discipline. His work on bureaucracy has been tremendously influential in contemporary surveillance theory, as elsewhere. Two aspects of Weber's theoretical project in particular have been central to sociological interpretations of contemporary surveillance practices. The first is Weber's focus on the theme of rationality as a feature of Western industrialization, and the second is his analysis of bureaucratization as an instance of the rationalization of human activity.[21]

Several parallels may be drawn between military organization and the modern bureaucratic form. Like the military, modern bureaucracies function on the principle of "fixed and official jurisdictional areas, which are generally ordered by rules, that is, by laws or administrative regulations."[22] Furthermore, Weber notes that, like military authority, bureaucratic authority is constituted by three principal elements:

> 1. The regular activities required for the purposes of the bureaucratically governed structure are distributed in a fixed way as official duties.
> 2. The authority to give the commands required for the discharge of these duties is distributed in a stable way and is strictly limited by rules concerning the coercive means, physical, sacerdotal, or otherwise, which may be placed at the disposal of officials.
> 3. Methodical provision is made for the regular and continuous fulfillment of these duties and for the execution of the corresponding rights; only persons who have generally regulated qualifications to serve are employed.[23]

Bureaucracy, as it is constituted by these three elements, only became fully developed in the context of the modern state, for it is within this context that the administrative functions of government have undergone tremendous growth. Lyon argues that modern surveillance societies are characterized by extensive administration, and traces what he sees as bureaucratic *excess* to this growth of administrative

---

[21] Gandy, op cit., pp. 7.
[22] Max Weber, *Bureaucracy*, From Max Weber: Essays in Sociology. H.H. Gerth and C. Wright Mills, eds. (New York: Oxford University Press, 1958) pp. 196.
[23] Ibid., pp. 196.

functions in the twentieth century. In the nineteenth century, notes Lyon, burgeoning nation-states searched for ways of carrying out their growing administrative responsibilities. Over time, functions such as taxation, property registration, the gathering of demographic information, voter registration, and conscription became increasingly bureaucratized.

The relationship between bureaucratization and the growth of surveillance societies is, at some level, an explicit one, for bureaucratic authority is based on the creation and maintenance of written documents or files which, in practice, serve to establish regimes of dataveillance. According to Weber, the success of bureaucracy lies in its ability to optimize effectiveness through "precision, speed, unambiguity, knowledge of the files, continuity, discretion, unity, strict subordination, reduction of friction and of material and personal costs..."[24] As a technology of organization, bureaucracy is information-intensive and thus contributes subtly to the normalization of surveillance. Through the experience of dealing with bureaucracy, people become habituated to providing various kinds of information, and especially personal information, as part of the process of acquiring or using goods and services.[25]

In a contemporary context, bureaucratization has led to the expansion of surveillance through data matching or data linking schemes. The vast information holdings of government bureaucracies, which are increasingly stored in electronic form, make such initiatives relatively easy to carry out. Through such schemes, information collected for a particular purpose by one department or organization is matched with the data collected for other purposes or by other departments, thereby creating a more complete surveillance profile. Commonly, data linking initiatives are undertaken in the hopes of catching individuals who are defrauding the government by claiming welfare or other benefits to which they are not entitled. In British Columbia, for example, such initiatives have been undertaken by a number of ministries, and have generally met with public support.[26]

---

[24] Ibid., pp. 214.

[25] This can be seen in a variety of everyday contexts. Radio Shack and Consumer's Distributing, for example, ask for the name, address, and telephone number of anyone making a purchase. Anecdotal evidence would seem to suggest that few people ever question these practices or refuse to provide the information.

[26] Such initiatives have been undertaken, for example, by the Ministry of Social Services in the context of efforts to curb welfare fraud. British Columbia's new Pharmanet system is also, in some sense, a data-matching scheme. The system links the prescription records of all B.C.

Part of the success of bureaucracy as an administrative technology has clearly been its ability to maximize self-reporting by providing various services and benefits in exchange for information or, alternatively, to punish failure to report. The emergence of bureaucratic authority as a mechanism for administering the business of the state has played a major role in the emergence of the state as a principal nexus of surveillance activity. Modern surveillance societies, however, are characterized by widespread systematic surveillance which extends far beyond the parameters of the state. The historical emergence of capitalism, and of the capitalist business enterprise more specifically, has been the single most important factor in the development of surveillance structures outside the state. Of particular significance has been the emergence of surveillance as a feature of workplace organization through the mechanism of management, and the development of surveillance structures that monitor and manipulate patterns of consumption.

Disciplining the Worker: Management as Social Control

Historically, the emergence of new relations of production under capitalism created a demand for new forms of discipline. Under feudalism, discipline had been achieved primarily through physical coercion and local, familial, and religious structures. But the historical development of the bourgeoisie, argues Marx, put an end to all "feudal, patriarchal, idyllic relations...[The bourgeoisie] has pitilessly torn asunder the motley feudal ties that bound man to his 'natural superiors,' and has left no other nexus between man and man than naked self-interest, than callous 'cash payment.'"[27] Exploitation ceases to be veiled under "religious and political illusions" and becomes "naked, shameless, direct, [and] brutal."[28] "[L]abourers, who must sell themselves piece-meal, are a commodity, like every other article of commerce, and are

---

residents. The records can then be accessed from any pharmacy in the province. Pharmanet was ostensibly designed to prevent patients from obtaining the same prescription from different physicians, and to prevent dangerous mixing of incompatible prescriptions. While B.C.'s Information and Privacy Commissioner and others were vocal and active in their condemnation of the scheme, the public seemed generally complacent. There are informal reports that the password option, which makes if difficult for pharmacists to access patient records without their knowledge or consent, is rarely used.

[27] Karl Marx and Friedrich Engels, *Manifesto of the Communist Party* in Robert C. Tucker, ed. The Marx-Engels Reader: Second Edition. (New York and London: W.W. Norton and Company, 1978, pp. 475.

[28] Ibid.

consequently exposed to all the vicissitudes of competition, to all the fluctuations of the market."[29] Although "live only so long as they find work, and ... find work only so long as their labour increases capital,"[30] still, an appearance of a choice must be maintained in order to preserve social stability. Workers must be able to imagine that they are free to choose how they use their labour power. The development of new disciplinary structures under capitalism is an important element in maintaining this appearance.

The need for discipline in the capitalist workplace, then, involves not simply controlling labour, but controlling *alienated* labour. Marx argued that "owing to the extensive use of machinery and to division of labour, the work of the proletarians has lost all individual character, and consequently all charm for the workman. He becomes an appendage of the machine, and it is only the most simple, most monotonous, and most easily acquired knack that is required of him."[31] The lack of responsibility or autonomy in the workplace evokes in the worker a sense of alienation; labour, which Marx contends should serve to "widen, to enrich, to promote the existence of the labourer,"[32] becomes a fundamentally dehumanizing and alienating experience under capitalism. This leads Marx to suggest that

> the fully formed proletariat represents, practically speaking, the complete abstraction from everything human, even from the *appearance* of being human; since all the living conditions of contemporary society have reached the acme of inhumanity in the living conditions of the proletariat; since in the proletariat man has lost himself, although at the same time he has both acquired a theoretical consciousness of this loss and has been directly forced into indignation against this inhumanity by virtue of an inexorable, utterly unembellishable, absolutely imperious *need*, that practical expression of *necessity* -- because of all this the proletariat itself can and must liberate itself.[33]

As a natural nexus of class antagonism and struggle, then, the workplace became an important site for disciplinary strategizing. In such a context, discipline in the workplace

---

[29] Ibid., pp. 479.
[30] Ibid.
[31] Ibid. Barbara Garson's interviews with employees of McDonald's and other large service-oriented companies would seem to suggest that, in some instances at least, this is an apt description of modern work conditions. As one employee notes: "You follow the beepers, you follow the buzzers and you turn your meat as fast as you can...[Y]ou don't need a face, you don't need a brain. You need to have two hands and two legs and move 'em as fast as you can. That's the whole system." Barbara Garson, The Electronic Sweatshop. (New York: Simon and Schuster, 1988) pp. 20.
[32] Ibid., pp. 485.
[33] Marx, *Alienation and Social Classes*, in Robert C. Tucker, ed. pp. 134.

served as a vehicle through which the threat of revolution or rebellion could be circumscribed, as well as being an instrument of internal pacification by which the worker becomes habituated to the capitalist mode of production. Thus management has been, at one level, the mechanism through which class relations within the capitalist business enterprise are channeled and ordered.

While discipline in the workplace has clearly had certain constraining effects in terms of its role in controlling labour, it has also had certain enabling functions. In particular, workplace discipline, which includes not only the various written and unwritten rules of an organization, but also its corporate culture and the various often subtle ways in which certain behaviours are punished or rewarded,[34] has the effect of streamlining the efforts of individual workers so that all are working toward the achievement of the same organizational goals. While these goals will generally include the maximization of profit, they may also include other goals, such as the provision of high levels of customer service, rapid technological innovation, or socially responsible business practices. Workplace discipline, then, serves to provide labour with a certain continuity and coherence in terms of organizational goals. It is in this sense that workplace discipline can be understood as enabling, rather than simply constraining, certain behaviours.

Closely related to the managerial imperative to maximize profit have been projects aimed at increasing productivity, which is measured as output per hour of work or time expended. Traditionally, the United States has boasted the world's highest levels of productivity. Although other countries have now surpassed the United States in this domain, the U.S. remains the birthplace of a number of profoundly influential management techniques. Over the course of the past century, many of these techniques have passed in and out of fashion. But the concern with productivity levels has endured. In practice, efforts to increase productivity have generally entailed the development of structures of supervision and surveillance, since such efforts have been largely concerned with the "timing, placing, observing, and checking of work."[35]

The link between attempts to increase productivity and surveillance has historically been mediated by two components of American management techniques in

---

[34] See, for example, Bergquist, op. cit., on shaming.
[35] Lyon, op. cit., pp. 34.

particular: time study, or work measurement, and wage payment. Both of these components have involved the setting of standards for productivity, and the subsequent development of measures to ensure that standards are met. Since these structures almost inevitably involve methods of monitoring work, the link between management techniques and surveillance has been made explicit here. This link has its roots in the principles of scientific management developed by Frederick Taylor in the early 1900's. Although scientific management has long been out of vogue, many of its principles have been incorporated into standard managerial practice. Certain aspects of Taylor's work remain relevant today as businesses continue to face pressures to maximize efficiency and increase productivity.[36]

Time study, or work measurement, is considered to be the cornerstone of scientific management, and it continues to be relevant in contemporary work contexts. Frank and Lillian Gilbreth were the founders of modern motion study techniques, which involve establishing an allowed standard time to perform a particular task based on a measurement of the work content and the prescribed method of performing the task. "Time study analysts use several techniques to establish a standard: a stopwatch time study, computerized data collection, standard data, fundamental motion data, work sampling, and estimates based on historical data."[37] Surveillance is implicated in this project in a number of ways. In the first instance, surveillance and work monitoring are used to gather information about specific tasks. These tasks are broken down into component parts and analyzed in minute detail. Once the task has been thoroughly analyzed and understood, managers then determine the most economical ways in which to perform the task, thereby improving efficiency. Using this "efficient ideal" as a model, managers determine what production norms and averages are and should be, and set production goals and performance requirements. Clearly, then, the organization of schemes of work under scientific management is reliant upon the ability to watch, record, measure, and compare detailed information about particular tasks.

The role of surveillance extends beyond the initial establishment of schemes of work, however, for surveillance is the mechanism through which adherence to these

---

[36] William K. Fallon notes that "[T]o compete successfully in world markets, [American managers] will have to do three things -- and do them well -- in the decades ahead. These are managing complexity, adaptation, and productivity." In W.K. Fallon, ed., AMA Management Handbook (Second Edition). (New York: Amacom, American Management Association, 1983) pp. I-25.
[37] Niebel, p. cit., pp. 7.

schemes is verified. Continuous monitoring ensures that workers conform to set labour processes and strive to meet the production and performance goals determined by management. At the same time, surveillance functions to reproduce hierarchical relations between management and labour in the workplace, reinforcing the role of management as the only legitimate source of knowledge about work and work processes. The technologically-enhanced eyes of management have the capacity to see everything on the shop floor; no detail is too small to escape the notice of electronic monitors, video cameras or computer equipment. In this way, labour is further disassociated from the labourer, the unpredictability of the 'human element' is greatly reduced, and the achievement of maximum efficiency becomes possible.

It is worth noting that, although the literature on surveillance has been rather inattentive to changes in management philosophies, and has tended to remain focused on traditional management styles such as scientific management and time study, changes in the culture of management will clearly have an impact on the role of[38] surveillance in the workplace. In more contemporary organizations, with their relatively flattened hierarchies and their less adversarial style of human resources management, surveillance is perhaps more likely to exist as a *potential* rather than an actual practice. In such environments, the potential for surveillance is probably enough to ensure a certain degree of self-censorship and self-surveillance in a way which does not have adverse of obvious effects on corporate culture and workplace relations.[39] The role of surveillance in these types of organizations is clearly a topic that warrants some careful study.

The focus in the surveillance literature on more traditional management techniques is misleading, then, because it implies that the new technologies of surveillance are simply being applied to old management problems. As I suggested

---

[38] There are a great many books on contemporary management trends. See, for example, Henry Mintzberg, Mintzberg on Management: Inside our Strange World of Organizations. (New York: The Free Press, 1989); Peter Drucker, Managing in a Time of Change. (New York: Turman Talley Books/Dutton, 1995); Jay Shafritz and J. Steven Out, Classics of Organization Theory (Fourth Edition). (Florida: Harcourt Brace College Publishers, 1996); William Bergquist, The Postmodern Organization: Mastering the Art of Irreversible Change. (San Francisco: Jossey-Bass Publishers, 1993); and Derek F. Pugh et al., Writers on Organizations (Fifth Edition). (Thousand Oaks: Sage Publications, 1996).

[39] Contemporary organizations may also opt for strategic e-mail privacy in order to encourage employees to use e-mail as a tool of professional development and to foster closer bonds between colleagues, customers and suppliers.

previously, this may well be the case in some organizations, but these organizations are not necessarily representative, nor are they likely to indicate the future path of workplace surveillance. As Hammer and Champy note, the successful corporation is not one which uses new technologies to solve old problems, but one which uses new technologies to create new opportunities.[40] The failure of the literature on surveillance to deal adequately with emerging managerial discourses is indicative, perhaps, of the lack of dialogue between theorists of surveillance and actual users, or potential users, of surveillance technologies.

Whatever changes have occurred in management styles, however, the drive to maximize profit endures, and has continued to be expressed in a number of ways, including the desire to increase productivity by reducing uncertainty about the 'human element' in production. This has resulted in the expansion of disciplinary structures well beyond the parameters of the workplace. Thus, as I noted previously, employers have grown increasingly interested in collecting personal, non-work related information about their employees, as well as their customers. In each case, the information is collected in order to generate certainty about human behaviour, either as an employee or as a consumer. While the collection of personal information about employees has long-standing roots in the tradition of Fordism, consumer surveillance is a somewhat newer phenomenon, with roots in the works of Alfred Sloan of General Motors.

Eyes on the Market: The Evolution of Consumer Surveillance

The rapid and tremendous growth of consumer surveillance reflects the emerging role of consumption as the primary locus of identity and social significance under conditions of late or high capitalism.[41] Consumption has arguably become the "all-absorbing, morally-guiding, and socially integrating feature of contemporary life in

---

[40] Michael Hammer and James Champy, *Reengineering the Corporation: the Enabling Role of Information Technology*, Classics of Organization Theory (Fourth Edition). Jay Shafritz and J.Steven Out, eds. (Florida: Harcourt Brace Publishers, 1996).

[41] Ernest Mandel notes that the term 'late capitalism' may be somewhat misleading because "it is one of chronology, not of synthesis...'late capitalism' in no way suggests that capitalism has changed in essence...The era of late capitalism is not a new epoch of capitalist development. It is merely a further development of the imperialist, monopoly-capitalistic epoch. By implication, the characteristics of the imperialist epoch enumerated by Lenin thus remain fully valid for late capitalism." See Ernest Mandel, Late Capitalism. (London: Verso, 1978) pp. 9.

affluent societies."[42] As Gandy argues, we are moving toward a situation where social order is enacted through hierarchies of consumption which are mediated through consumer surveillance. The coercive mechanisms through which the nation-state has traditionally maintained social order continue to be relevant, though perhaps more so for those subjects who are marginalized in or by consumer culture. In such a context, data about consumers and their patterns of consumption is a commodity in itself. The value of this commodity increases in direct proportion to the amount of detail that can be obtained about the number of units sold, the price, the advertisement that spurred the sale, and the people who bought the product. "Information about their own customers takes on a new value as the technology of database marketing makes it possible for firms to target their promotions to those most likely to respond to similar appeals in the future."[43]

It has been suggested that consumer surveillance can be understood as a form of social management. Kevin Robins and Frank Webster, for example, argue that consumer surveillance is an extension of Taylorism into the social sphere.[44] As such, it calls attention to the ways in which power functions through management and all of its various techniques which include, but are obviously not limited to, techniques of surveillance. The functioning of power is clearly apparent in the structuring of consumer surveillance. This same type of power is to be found in conditions of workplace surveillance, where it is wielded by management as a mechanism with which to discipline workers. Thus is it worthy of at least brief consideration here.

During the 1920s, Alfred Sloan applied the principles of scientific management to consumer behavior, using information about buying habits to develop customer profiles. A similar process was undertaken by the Spiegel Corporation in the mid-1930s as a way of evaluating credit applications. Spiegel developed a series of 'vital questions' which were used to determine whether applicants would be granted credit. These questions pertained to the dollar amount of the order, the occupation of the applicant, marital status and race.[45] Modern forms of market research and credit reporting, with their emphasis on detailed consumer information, have their roots in these practices. Such

---

[42] Lyon, op. cit., pp. 137.
[43] Gandy, op. cit., pp. 62.
[44] Frank Webster and Kevin Robins, *Plan and Control: Towards a Cultural History of the Information Society*. Theory and Society. 1989, pp. 18.
[45] Ibid., pp. 1.

practices have tremendous social significance, for they are intimately linked to the establishment of hierarchies of consumption and the resulting social order. In this sense, consumer surveillance can be said to have disciplinary effects. Thus the context in which consumer surveillance has taken place is a highly politicized one which has important social ramifications.

Taken together, the development of surveillance structures in the military, bureaucracy, and capitalist business enterprise have provided fertile grounds for the emergence of modern surveillance societies. Such societies, as we have seen, have been characterized by their development of elaborate surveillance structures in response to problems of discipline and rationalization. These structures, by and large, have served to entrench pre-existing patterns of power distribution, rather than to undermine or compromise them. This is the context in which contemporary surveillance practices, such as the monitoring of employee e-mail, must be considered. For these practices clearly do not emerge in a vacuum, but rather reflect and participate in larger and more generalized historical movements.

A New Surveillance?

It seems that, in the modern age of automated banking, electronic messaging, automatic debiting, and smart cards, or lives are subjected to closer and closer scrutiny by an increasingly wide array of interested parties. There is some question as to what this apparently growing scrutiny means, both at the level of the individual and in a more general sense.[46] For some analysts, Foucault's work on Bentham's Panopticon sheds some insight on these questions, and the metaphor of Panopticism has increasingly captured their imaginations. Panopticism, as defined by Foucault, is the "general principle of a new 'political anatomy' whose object and end are not the relations of

---

[46] I am indebted to Colin Bennett for pointing out to me that there is an argument to be made that surveillance is not, in fact, growing. In feudal times, for example, peasants lived under conditions of fairly extensive and intrusive surveillance. Nevertheless, I would argue that the proliferation of opportunities for interaction in the modern age has created opportunities for more extensive surveillance, and also for an increase in the number of parties carrying out the surveillance. Thus, for example, personal information can be generated, collected, and used when we borrow books from the library, rent a video, use credit cards, make long-distance telephone calls, buy things with our bank cards, or subscribe to a magazine. In a contemporary context, then, surveillance can generate information not only about what we *do*, but also about who we *are*.

sovereignty but the relations of discipline."[47] He sees in Bentham's prison design a "generalizable model of functioning; a way of defining power relations in terms of the everyday life of men."[48] And while Foucault himself never addressed the relationship between emerging electronic surveillance practices and the Panopticon, his work seems to have significant applications in this field. It is perhaps a sign of the growing concern and alarm about electronic surveillance, and especially about dataveillance, that the image of the Panopticon, with its inescapable visibility, has become such a powerful metaphor for surveillance societies.

Bentham's original panoptic design was based on a central watch tower with single-person cells fanning out around it in a circle. Backlighting and carefully-angled blinds would make it possible to see clearly into every cell from the watchtower. At the same time, these same features would ensure that the supervisor would be invisible to the inmates. As a result, inmates could never be certain of whether they were being watched at any given moment. This uncertainty would be the basis of their subordination, for the inmates would have no choice but to believe that they were *always* being watched. In this way Bentham built the notion of omniscience into his secular scheme for moral reform.

While the principle of inspection was clearly the cornerstone of Bentham's design, classification also played an important role. Despite the fact that prisoners were to be kept in solitary cells, Bentham also insisted that they be clearly classified and segregated by category in order to avoid the dangers of association. Lyon notes that, in one of his plans, Bentham proposed to divide inmates according to whether they were ""Thoroughbred Housebreakers, Quiet Old Offenders, Decent Females, Dissolute Females" and so on."[49]

In essence, then, the principles of Bentham's design -- inspection, solitude, and classification -- would guarantee order by making the inmate "the object of information, [but] never a subject in communication."[50] These principles clearly held a certain amount of appeal, for while Bentham was never successful in selling the Panopticon to

---

[47] Michel Foucault, Discipline and Punish: The Birth of the Prison. (New York: Vintage Books, 1979) pp. 208.
[48] Foucault, pp. 205.
[49] David Lyon, *Bentham's Panopticon: From Moral Architecture to Electronic Surveillance*, Queen's Quarterly 98/3 (Fall 1991) pp. 600
[50] Foucault, pp. 200.

the British, Panoptic principles found expression in the design of many nineteenth century prisons, factories, schools, workshops, barracks and hospitals in Europe and North America.[51] The appeal of panoptic principles must lie, at least in part, in the fact that the Panopticon serves as a distinctly modern disciplinary machine -- continuous, impersonal, and automatic in its functioning. Indeed, the Panopticon signaled for Foucault the transition between the old regime, where discipline was achieved through threatened or actual physical punishment and torture, and modernity, where subtle shifts in the pain-pleasure calculus are used to alter or "reform" behaviour.

In Foucault's analysis, the Panopticon emerges as the architectural figure of the merging of the projects of exclusion and discipline which have their roots in the leper and the Plague, respectively . This merging of the two projects did not occur until the nineteenth century, when the Panopticon combined them by applying the technique of power proper to disciplinary partitioning to the space of exclusion of which the leper was the symbolic inhabitant.[52] Thus the inmates in the panoptic prison are ordered in such a way as to ensure that "each actor is alone, perfectly individualized and constantly visible."[53] The major effect of the Panopticon, then, and its genius, is that it assures the automatic functioning of power by suspending the inmates in a state of conscious and permanent visibility. The fact of being permanently visible does away with the need for constant supervision, for "the surveillance is permanent in its effects, even if it discontinuous in its action," leading Foucault to comment that "the perfection of power should tend to render its actual exercise unnecessary."[54] In the context of the Panopticon, then, power functions by being at once visible, in that each inmate can see the tower from their cell, and unverifiable, in that they can never be sure whether they are being watched at any moment.

The state of conscious and permanent visibility which is achieved in the Panopticon has the important effect of inducing inmates to monitor themselves. As Foucault notes: "He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own

---

[51] Lyon, "Bentham's Panopticon," pp. 597.
[52] Foucault, pp. 199-200.
[53] Ibid., pp. 200.
[54] Ibid.

subjection."[55] In this way, the inmates of the Panopticon come to be disciplined in a very fundamental and powerful way; the possibility of disobedience is extinguished and, with it, the very thought of it. As Bentham himself observed, "[t]o be incessantly under the eyes of the inspector is to lose in effect the power to do evil and almost the thought of wanting to do it."[56]

It is as a result of its ability to create real subjection from a fictitious relation that the Panopticon can be regarded as more than a design for a prison building. Rather, it is more aptly regarded as "the diagram of a mechanism of power reduced to its ideal form; its functioning, abstracted from any obstacle, resistance or friction, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use."[57] As a mechanism of power, the Panopticon functions to concentrate power by reducing the number of people required to exercise it while maximizing the number of people it is exercised on. Panoptic power is also preventative; its "constant pressure acts even before the offenses, mistakes or crimes have been committed."[58] At the same time, the functioning of panoptic power is spontaneous and silent, acting directly upon the individual.

The Panopticon, with some slight modifications, clearly has applications in a wide variety of contexts. Foucault notes that the panoptic schema can be integrated with any function in order to increase the effect of that function. In Foucault's words, the panoptic schema is "a way of making power relations function in a function."[59] As such, the Panopticon does away with the cumbersome and rigid exercise of power from the outside, replacing it with a subtle, continuous and automatic functioning. Given these features, it is not surprising that Foucault proclaims that the panoptic schema "was destined to spread throughout the social body; its vocation was to become a generalized function."[60] As a generalized function, the Panopticon has a role of amplification; "although it arranges power, although it is intended to make it more economic and more effective, it does so not for power itself, nor for the immediate salvation of a threatened society: its aim is to strengthen the social forces - to increase production, to develop the

---

[55] Ibid., pp. 202-3.
[56] Lyon, op. cit., pp. 597.
[57] Ibid., pp. 205.
[58] Ibid., pp. 206.
[59] Ibid., pp. 206-7.
[60] Ibid., pp. 207.

economy, spread education, raise the level of public morality; to increase and multiply."[61]

In this way, the Panopticon replaces the relations of sovereignty with the relations of discipline. As the design of Bentham's prison makes clear, continuous or seemingly continuous surveillance plays an important role in securing these relations. What has been significant about Foucault's work, then, is that is has sensitized at least some surveillance theorists to the ways in which power functions through surveillance, reproducing and amplifying existing social patterns. At the same time, Foucault's work highlights the fact that disciplinary systems like the Panopticon discipline *subjects*. Thus we find in Foucault's work a reason to take the theme of subjectivity seriously when considering the effects of surveillance.

Foucault's work, then, provides one way of getting at the question of whether contemporary surveillance practices break so significantly with older forms of surveillance that they can be considered to be new. This question has been a central one for many theorists. While some, like James Rule, have argued that there is a great deal of continuity between older and newer forms of surveillance, others maintain that modern technologies, and especially electronic technologies, change the character of surveillance so fundamentally that it is, indeed, new. David Lyon and Gary Marx, for example, argue that the widespread use of microelectronic technologies has extended the role of surveillance, which was conventionally a function of policing, so that we are approaching "maximum security societies" in which the relationship between surveillance and social control is increasingly explicit.[62] In such societies surveillance power is extended to the producers of hegemonic culture and to other holders of social, political, and economic power.

In making his case for the recognition of a new surveillance, Marx identifies nine distinctive attributes of the new surveillance.[63] The first is that it transcends distance, darkness, and physical barriers, making use of technology to gain access to the "inner

---

[61] Ibid., pp. 208.

[62] Gary Marx, Undercover: Police Surveillance in America. (Berkeley: University of California Press, 1988) pp. 232.

[63] These nine distinctive attributes appear repeatedly in Marx's work. The discussion of these attributes that follows is taken from Gary Marx, *The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures*, in James F. Short, Jr., ed. The Social Fabric: Dimensions and Issues. (Beverly Hills: Sage, 1986) pp. 149-153 and from *I'll Be Watching You: Reflections on the New Surveillance*, in Dissent 22: pp. 26-34.

intellectual, emotional, and physical regions of the individual."[64] Traditionally, one could reasonably expect one's activities to be shielded by distance, darkness, or physical barriers. New technologies, however, render such shields virtually irrelevant. "Sound and video can be transmitted over vast distances, infrared and light-amplifying technologies pierce the dark, intrusive technologies can "see" through doors, suitcases [and] fog."[65] As a result, the notion of a private space is becoming increasingly ambiguous.

A second attribute of the new surveillance is that it is able to transcend time by creating records that can be easily stored, retrieved, combined, analyzed, and communicated either immediately after collection or much later, in a variety of interpretive contexts. Information is stored in forms that make it portable, easily reproducible, and transferable across vast distances. This facilitates massive scale data-sharing and data-matching projects, which collate and cross-reference information from various sources, thereby providing the opportunity to create a more complete surveillance profile.

Another distinctive attribute of the new surveillance is that it is capital- rather than labour-intensive. This has a profound effect on the economics of surveillance, making surveillance considerably less expensive on a per unit basis than it has traditionally been. Economies of scale can be achieved by transmitting data back to a central source, enabling a few people to monitor many people and places simultaneously. Further economies may also be achieved as a result of increased self-surveillance.

The fourth distinctive feature of the new surveillance is that, according to Marx, it triggers a shift from targeting a specific suspect to categorical suspicion. "The camera, the tape recorder, the identity card, the metal detector, the obligatory tax form that must be filled out even if one has no income, and the computer make all who come within their province reasonable targets for surveillance."[66] While some might argue that these devices are "soft" forms of surveillance, they are nevertheless insidious and permit continuous rather than intermittent monitoring. This type of surveillance functions on the assumption of guilt and fosters a society where suspicion is the norm.

---

64 Gary Marx, *The Iron Fist*, pp. 150.
65 Marx, *I'll be Watching You*, pp. 30.
66 Marx, *The Iron Fist,* pp. 150.

Another distinguishing feature of the new surveillance is that it is principally concerned with the prevention of violations. It is, in part, an anticipatory strategy which attempts to make social control more predictable, and consequently more reliable and effective. This strategy clearly betrays its roots in the bureaucratic project of rationalization, which is also a significant feature of modern management. Of course, even total surveillance cannot guarantee one hundred per cent predictability. "Where violations cannot be prevented, the surroundings may be so structured that violators are either caught in the act or leave strong evidence of their identity and guilt."[67]

The new surveillance is also distinguished from older forms by the fact that it is decentralized. Marx argues that "in contrast to the trend of the last century, information can now in principle flow as freely from the center to society's periphery as the reverse. National data resources are available to widely dispersed local officials."[68] This trend triggers self-policing as the surveillance is often self-activated and automatic, for example when people sign a book out of the library, obtain a driver's permit, or fill out a contest entry form.

Significantly, the new surveillance is also either invisible or has low visibility. As a result, it becomes increasingly difficult to know whether or when one is being watched and by whom. Marx argues that "there is a distancing (both socially and geographically) between watchers and watched, and surveillance is increasingly depersonalized."[69] Furthermore, the instruments of surveillance -- video cameras, recorders, one-way mirrors and so on -- are often well-hidden. Dataveillance, which is an increasingly common form of surveillance, is perhaps even more difficult to trace since the information that we provide on an almost daily basis for a variety of purposes, such as our name, address, or phone number, seems inevitably to reappear in apparently unrelated contexts.

Finally, the new surveillance is more intensive than its predecessors, collecting information that was previously inaccessible. "With blood and urine analysis and stomach pumps it "sees" into the body -- and with voice stress and polygraph analysis it attempts to "see" into the soul, claiming to go beneath ostensible meanings and appearances to real meanings. At the same time, surveillance has become more

---

67 Ibid.
68 Ibid., pp. 151.
69 Ibid.

extensive. "Broad new categories of person and behaviour have become subjects for information collection and analysis, and as the pool of persons watched expands, so does the pool of watchers. Anyone may be watched: everyone is a potential watcher."[70] The expansion of surveillance, combined with its increasing invisibility, makes possible a strategic uncertainty which allows the disciplinary or social control function of surveillance to operate even when no actual surveillance is taking place.

While Marx's delineation of the characteristics of the new surveillance may well be persuasive, it does not, in my opinion, manage to address the question of why the debate about the newness of surveillance is important. The categories of new and old, particularly when they are linked to the state of technological change, do not strike me as being particularly interesting or useful in this case. Marx's argument fails to address the ontological questions that I take to be absolutely fundamental to understanding the nature of surveillance, new or old. Thus the interesting question, for me, is not whether surveillance is new (or old), but whether *subjects are constituted differently* under modern conditions of surveillance. This framing of the question moves away from a concern with the various practices that make up surveillance societies and instead focuses attention on the context in which surveillance occurs, and the subjective effects of both that context and the surveillance more generally. Such a framing is in line with the political analysis of surveillance as an instance of the functioning of power which is suggested by Foucault.

Conclusion

The path along which surveillance has developed in modern societies, and in particular how the themes of discipline and rationalization have been played through the development of surveillance structures in military, bureaucratic, and capitalist workplace settings, would certainly seem to support the suggestion that the development of surveillance societies has had important implications at the level of subjects. Indeed, it seems clear that contemporary surveillance practices *must* constitute subjects in different ways, because it is precisely their intention to do so. These surveillance

---

[70] That everyone is a potential watcher is evidenced, for example, by the enduring popularity of television programs such as America's Most Wanted and Crimestoppers, which encourage citizens to watch one another and to report suspicious activity. Such programs highlight not only the new sources of surveillance, but also the apparent appeal of being a watcher or voyeur.

practices are heavily invested in disciplining subjects in such a way as to produce and reproduce social order, as well as to render behaviour predictable in a variety of productive and consumptive contexts. This point may seem rather banal, but it is one which has been largely lost or forgotten in the literature on surveillance. The focus on technology and technological change which has characterized so much of that literature has pushed this kind of contextual analysis aside. And yet such an analysis is clearly crucial, for it provides a framework within which to consider the social, economic, and political causes and effects of surveillance at both the micro and macro levels.

The failure of the literature on surveillance to take seriously the full context in which surveillance operates is reflected in the extent to which the dominant analytical approaches to fail to consider the questions of subjectivity that are at stake in modern surveillance practices and in surveillance societies more generally. In the next chapter, then, I consider each of these analytical approaches in turn and show how it has problematized surveillance. Here I am particularly interested in highlighting the ways in which these literatures have asked, or failed to ask, practical and theoretical questions about what it means to say that we live in a surveillance society. Thus I consider whether these approaches are able to address widespread patterns of surveillance and their social effects, or whether they see each instance of surveillance as more or less isolated, bearing no connection to the larger context which I have sketched in this chapter.

Chapter Three: Theorizing Surveillance

The monitoring of employee e-mail is but one instance of surveillance in the workplace. Consequently, it must be situated within the larger patterns of surveillance that have come to characterize modern workplaces. These patterns, in turn, can be situated within the widespread and generalized surveillance structures which are integral features of modern forms of social organization. Surveillance structures in general, and certain surveillance practices in particular, became a focus of interest among academics and others during the 1960's. At that time, concerns about the social and political effects of surveillance were brought to the forefront by the development and application of computer and telecommunications technologies. These concerns were channeled into and expressed by an emerging literature that attempted to document, account for, explain, and predict the social, political, and economic effects of these new technologies and the surveillance potential associated with them.

The literature around surveillance, then, is a relatively young one. In practice, it has tended to be dominated by three principal theoretical approaches: the legal approach, the technological approach, and the sociological approach. These approaches can be roughly distinguished from one another by the way in which they problematize surveillance. Thus the legalistic literature has tended to view the problem as one of privacy and the loss of privacy.[1] The technological literature, by contrast, has framed the problem as one of anonymity and data security. Finally, the sociological literature has framed the problem as one of social control.[2]

---

[1] What I refer to here as the "legal literature" includes not only the relevant legislation and case law, but also the significant theoretical literature which has grown around the legislation.

[2] Like all classification schemes, this one has its flaws and its ambiguities. Some of the writing on surveillance does not fit very neatly into this scheme. David Flaherty, for example, is an historian, but he appears here as a legal theorist because his approach draws heavily on the legal tradition, and his emphasis is on privacy. Despite such ambiguities, I stand behind these categories as being useful and relevant ways of characterizing the literature on surveillance. They capture not only difference in how surveillance is problematized, but also differences in theoretical approaches to the question of surveillance more generally.

These three principal approaches reflect the primary sources of the academic literature on surveillance, and the centres where concerns about or interest in surveillance have been most clearly or urgently articulated. Legal theorists, technologists, and sociologists are invested in the debate around surveillance in different ways, and these are clearly reflected in the approach that each group has taken in framing the issues.[3] Interestingly, there has been little or no dialogue between these three major participants in the debate around surveillance. Part of my project here, then, is to bring to the forefront the silences that exist in contemporary discourses of surveillance and to consider what some of the effects of those silences have been.

In more general terms, this chapter focuses on the themes, questions, assumptions and silences that characterize contemporary literature on surveillance. While these are, in many ways, quite similar to the themes that have characterized public debates about workplace surveillance and, more particularly, the monitoring of employee e-mail, the academic discourse around surveillance has been not only more abstract, but also more in-depth. Clearly, many of the finer points of this discourse are lost or diluted in public debate. Thus this chapter seeks not simply to reiterate the themes of the last one, but to elaborate them, enrich them, and test their limits. I am not concerned, then, with reviewing, in careful detail, the full body of literature on surveillance. Others have already undertaken such projects, and I do not wish to reproduce their efforts here.[4] Instead, this chapter is primarily *thematic* in its approach, highlighting the shared concerns and assumptions that characterize the literature as a whole, and each approach in particular.

---

[3] While my focus here in primarily on the academic literature around surveillance, these same three approaches do seem to dominate the popular literature on that theme as well. In general, however, the popular literature has tended to be somewhat more alarmist than the academic literature, and has been more concerned with the loss of freedom, or the potential loss of freedom, associated with technologies of surveillance. See, for example, David Burnham, The Rise of the Computer State (New York: Random House, 1980), Jeff Rothfeder, Privacy for Sale (New York: Simon and Shuster, 1992), Ian Will, The Big Brother Society (London: Harrap, 1983), Duncan Campell & Steve Connor, On the Record: Surveillance, Computers and Privacy (London: Michael Joseph, 1986), Simon Davies, op. cit.

[4] Colin Bennett provides a particularly good review in The Political Economy of Privacy: A Review of the Literature. Hackensack: Center for Social and Legal Research.

Privacy: The Legal Discourse on Surveillance

The theme of privacy is a natural starting point for this review since, whatever differences may mark their approaches, legal theorists, technologists and sociologists have all arrived at the concept of privacy as the best response to the problems of surveillance. The foundations of the concept of privacy, and of the articulation of a *right* of privacy more specifically, are best be traced through the legal discourse around surveillance. Bennett has noted that "[t]here was much writing in the 1960's, particularly in American law journals, devoted to clarifying the privacy concepts for the purpose of setting some limitations to US tort and constitutional law."[5] These earlier writings continue to inform current work in the field, as is evidenced by the continuing focus on rights and the heavy reliance on the law to guard against surveillance that is deemed to be unfair.

Although privacy has, in many ways, been the cornerstone of the anti-surveillance literatures, it is a notoriously slippery concept, and there is little agreement in the literature as to what the right of privacy properly entails. Most often, claims to a right of privacy are entangled in claims about other rights, such as freedom and autonomy, as to be virtually indistinguishable from them. Thus it is not surprising that defining the relationship between privacy and other rights has been one of the major preoccupations of the legal discourse around surveillance. As part of this project, legal theorists have struggled with the difficulty of achieving a balance between privacy and other rights or obligations, such as social participation, which may conflict with privacy in certain circumstances. Despite the difficulty of articulating a clear place for privacy among these other rights, the claim to a right of privacy has been adamantly asserted and is central to the way the legal approach frames the problem of surveillance.

The ambiguity surrounding the concept of privacy and the nature of its relationship to other liberal values has required the development of a more precise concept around which to frame questions about surveillance; that of *information* privacy. The concept of information privacy shifts attention away from generalized philosophical debates about privacy and focuses it instead on particular problems

---

[5] Colin Bennett, *Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s*, Science, Technology, & Human Values. Vol. 16 No. 1, Winter 1991, pp. 58.

which are emerging, or have emerged, in the context of surveillance societies. In doing so, it moves from a conception of privacy as an aesthetic value, restricting personal information as an end in itself, to a conception of privacy as a strategic value, where personal information is restricted as a means to some other end.[6]

The limitation of the notion of privacy by way of the qualifier "information" has facilitated relatively widespread agreement concerning the parameters of information privacy as a concept. Bennett notes that "two very similar definitions of this right appeared at about the same time and had a widespread influence on the policy debates in different countries" -- Arthur Miller's and Alan Westin's.[7] Miller defines information privacy as the ability of individuals to control the circulation of information relating to them.[8] Similarly, Westin defines it as the claim of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others."[9] In this country, as in the United States, it is Westin's version that appears again and again in the literature on privacy and surveillance.

Westin's work has undeniably played a central role in shaping surveillance theory on this continent. Significantly, Westin has firm roots in the American legal tradition, and his work strongly reflects that tradition's emphasis on individualism, limited government, and private property. His definition of privacy suggests that it is not a *state*, but rather a *process* by which individuals regulate the boundaries between themselves and others. This highlights the extent to which the themes of autonomy, liberty, individuality, and intimacy underlie both his concept of privacy and the discourse of privacy more generally. At the same time, it draws attention to the critical relationship between the process of privacy regulation and the development and preservation of self-identity. The exploration of this theme signals an important bridge in the literature between the legalistic understandings of the *right* of privacy

---

[6] The theme of privacy as an aesthetic or strategic value is developed by James Rule et al. in The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. (New York: Elsevier, 1980), pp. 22.

[7] Ibid., pp. 59.

[8] Arther R. Miller, The Assault on Privacy. (Ann Arbor: University of Michigan Press, 1971) pp. 40.

[9] Alan F. Westin, Privacy and Freedom. (New York: Atheneum, 1967) pp. 7. This definition encompasses a notion of privacy as the right to be left alone, which was developed most influentially by Samuel Warren and Louis Brandeis in *The Right to Privacy*, Harvard Law Reveiw 4 (1890): 193-220.

and the psychological writing on the *function* of privacy in the development and presentation of self.[10]

The psychological functions of privacy are worth considering here in so far as they help to clarify what is understood to be at stake in debates about privacy and surveillance. In an article where he contemplates the concept of privacy, Irwin Altman suggests that it is fundamentally concerned with "(1) relationships between a person or group and others, (2) the interface of the self and others, and (3) self-definition and self-identity."[11] In the course of Altman's elaboration of these three functions, it becomes clear that self-identity is actually a precondition of the first two, which relate to the protection and limitation of communications between the self and others and evaluation of the self in relation to others, respectively. Both of these functions clearly require that a person have a sense of self-definition and self-identity -- a "cognitive, psychological, and emotional definition and understanding of himself [sic] as a being. [This understanding must include] knowing where one begins and ends vis-à-vis others, what aspects of the physical and social environment are parts of the self and which aspects are parts of others."[12]

For Altman, then, as for Westin, privacy is fundamentally concerned with the erection and patrolling of the borders of the self. The ability to choose between privacy and intimacy, between secrecy and disclosure is, for them, the ability to determine freely the parameters of the self as distinguished from the other. The possibility of making such a distinction rests in the unspoken though clearly important assumption that individuals are rational, mutually disinterested, self-identical subjects. Such subjects can be said to hold property in themselves. In such a context, privacy is about patrolling the clear but vulnerable borders of a

---

[10] One needs to be clear here; Westin argues that people have a *claim* to privacy, but does not specify that they have a *right* to it. Westin has been adamant in maintaining a distinction on this point. There are at least two difficulties with Westin's position, however. First, the assertion of a right to privacy *is* a kind of claim. If Westin is not claiming a right, then he needs to be more specific about what kind of claim it is that he is making. Second, in the American legal tradition, most claims eventually become framed as rights. So Westin would also need to be more specific about how or why the claim to privacy does not slide into becoming a claim to a right of privacy. On the tendency for claims to become rights, see Koopmans, op. cit.

[11] Irwin Altman, "Privacy: A Conceptual Analysis," Environment and Behaviour, Vol. 8 No. 1, March 1976, pp. 24.

[12] Ibid., pp. 25.

coherent and cohesive self. In this view, interactions between the self and others do not compromise or alter the "I" in any significant way.

From this perspective, it makes sense to distinguish between public and private selves, and between public and private spheres more generally. The ability to make this distinction has been central to the framing of privacy as a concept. Critiques of the public/private split are by now so common, at least among political scientists, that they are not worth going through in detail here. Certainly those critiques which have their basis in communitarian and/or feminist values have represented significant challenges to the assertion of the kind of public/private split that the discourse of privacy has been built on.[13] Such critiques have shown how profoundly that split reflects specifically modern ways of constructing the world. At the same time, these critiques have highlighted the violence implicitly in the construction of binary oppositions, which inevitably suspend the poles in a hierarchical relation. These criticisms have been met with a noticeable silence in the literature on privacy, and the public/private has remained central to how privacy is framed.[14]

---

[13] See, for example, Michel L. Walzer, Spheres of Justice (New York: Basic Books, 1983); Alasdair MacIntyre, After Virtue (Nortre Dame: University of Notre Dame Press, 1988) and Whose Justice? Which Rationality? (New York: Cambridge University Press, 1988); Michael J. Sandel, Liberalism and the Limits of Justice (New York: Cambridge University Press, 1982); Charles Taylor, "Cross Purposes: The Liberal Communitarian Debate" in Liberalism and the Moral Life, ed. Nancy Rosenblum (Cambridge: Harvard University Press, 1989); Virginia Held "Mothering versus Contract" in Beyond Self Interest. Jane J. Mansbridge, ed. (Chicago: Chicago University Press, 1990); Rita Manning, Speaking from the Heart: A Feminist Perspective on Ethics. (Maryland: Rowman and Littlefield, 1992); Nel Noddings, Caring: A Feminine Approach to Ethics and Moral Education. (Berkeley: University of California Press, 1984); Susan Moller Okin, Justice, Gender and the Family. (USA: Basic Books, 1989); Sara Ruddick, Maternal Thinking: Towards a Politics of Peace. (New York: Ballantine Books, 1989); Elizabeth Fraser et al., eds. Ethics: A Feminist Reader. (Cambridge: Blackwell, 1992), Marilyn Frye, The Willful Virgin: Essays in Feminism 1979-1992. (Freedom, California: The Crossing Press, 1992); Carol Gilligan, In a Different Voice: Psychological Theory and Women's Development. (Cambridge: Harvard University Press, 1982); Eve Browning Cole and Susan Coultrap-McQuin, eds. Explorations in Feminist Ethics: Theory and Practice. (Bloomington and Indianapolis: Indiana University Press, 1992); John Hardwig, "Should Women Think in Terms of Rights?" and Owen Flanagan and Kathryn Jackson, "Justice, Care and Gender: The Kohlberg-Gilligan Debate Revisited" in Feminism and Political Theory. Cass Sunstein, ed. (Chicago: University of Chicago Press, 1990); Carole Pateman, The Sexual Contract. (Stanford: Stanford University Press, 1988); Anita Allen and Erin Mack, "How Privacy Got Its Gender" Northern Illinois University Law Review 10: 441-78.

[14] The failure of the literature on surveillance to address the problematic of public/private

Robert Holmes' work is typical in this sense. He argues that the right of privacy is directly derived from the existence of an inner private realm which shields our true thoughts and feelings from others. This realm is paralleled by an external private sphere which has been traditionally associated with home and family. In essence, then, the public/private split is a reflection of the mind/body dualism that Holmes races through the writings of Plato and Mill. It is in this dualism, and in the valuing of mind *over* body in particular, that Holmes finds the basis of human freedom and the related values of autonomy and privacy.

While Holmes' purpose is ostensibly to show the foundations of the right of privacy, he is actually more successful at illustrating how difficult it is to distinguish privacy from other liberal values. He maintains, for example, that privacy can be distinguished from autonomy because the former is a *freedom* while the latter is a *capacity* to live as one chooses.[15] But further along in his analysis it becomes clear that his notion of privacy presupposes the existence of a certain measure of autonomy. Indeed, he argues that "privacy is freedom from unauthorized intrusion into areas of our lives not normally open to others, then except in rare circumstances -- such as those of a hermit or a person stranded on a desert island -- privacy depends upon our ability to control access to those areas."[16] In Holmes' schema, this ability is understood to be an aspect of autonomy.

In the final analysis, then, Holmes fails to be persuasive on two counts. First, his claim that the right of privacy flows from the existence of mind, and from the externalization of its characteristics in the private sphere, is a weak one, and does not address the process by which dualisms like mind/body and public/private are enacted. Second, although Holmes tries to show how privacy can be distinguished from autonomy, his argument has quite the opposite effect. Indeed, privacy seems to emerge from his analysis not as a right in itself, but rather as a component of autonomy. Holmes' attempt is instructive, however, because it illustrates the ambiguity of the concept of privacy and its relationship to other liberal values.

---

is perhaps a reflection of the virtual absence of political scientists in this field. Notable exceptions to this rule would include Priscilla Regan, Colin Bennett, and Charles Raab.

[15] Holmes, pp. 18.

[16] Ibid., pp. 19.

This same ambiguity is reflected in the legalistic literature on surveillance more broadly. David' Flaherty's extremely influential work in this area is typical in this way. In his book on protecting privacy in surveillance societies, for example, Flaherty claims that individuals have certain privacy interests in information about themselves. He lists those interests as follows:

- The right to individual autonomy
- The right to be left alone
- The right to a private life
- The right to control information about oneself
- The right to limit accessibility
- The right of exclusive control of access to private realms
- The right to minimize intrusiveness
- The right to expect confidentiality
- The right to enjoy solitude
- The right to enjoy intimacy
- The right to enjoy anonymity
- The right to enjoy reserve
- The right to secrecy.[17]

For my purposes here, Flaherty's list is significant in two ways. First, although Flaherty claims to be listing privacy interests, other liberal values, including autonomy, liberty, property, and individualism figure prominently in his list. These other values are clearly and profoundly implicated in Flaherty's conception of privacy, although the precise nature of the relationship between privacy and these other values is never articulated. In this sense, Flaherty conforms to a well-established pattern in the literature. Indeed, Bennett has made the point that liberal values such as the ones featured in Flaherty's table, are often subsumed under the rubric of privacy.[18] The prominence of autonomy, liberty, property and individualism in Flaherty's table of privacy interests would seem to confirm Bennett's analysis.

The second way in which Flaherty's table is significant is that, although it is identified as a table of *interests,* it is made up of as a series of *rights.* This suggests that the right of privacy is derived simply from having an interest in it. Such a move is characteristic of what T. Koopmans terms the "constitutionalization of rights," referring to the process by which legal discourse transforms interests into rights, and

---

[17] Flaherty, Protecting Privacy in Surveillance Societies, pp. 8.
[18] Bennett, *Computers, Personal Data, and Theories of Technology*, pp. 58.

rights into *fundamental* or *human* rights.[19] Koopmans notes that "[i]n 20th century thinking, almost every interest can be translated, especially by lawyers, into a right."[20]

The construction of privacy as a right is a recurring tendency not only in Flaherty's work, but also in the legalistic literature on surveillance more generally. The leap from asserting an interest in privacy to claiming a right of privacy is a slippery one, and it raises some interesting questions. As a strategy, the value of constructing privacy as a right rather than an interest is clear: rights are far more compelling, and carry greater weight than do interests. Furthermore, once a right is recognized, it will generally be protected, most often by law, whereas interests are unlikely to be afforded this kind of legitimacy.

The North American tradition of rights discourse has tended to be obsessed with the idea of justice as fairness. This tendency reflects the profound and lasting legacy of John Rawls, who used a veil of ignorance as the starting point for his theory of justice. This veil of ignorance is Rawls' foundational myth and its function is to render political and social differences invisible. Using this "clean slate" as a starting point, argues Rawls, rights and obligations can be rationally and fairly agreed upon. The reliance on traditional rights discourse in the context of debates about privacy and surveillance is one aspect of what Koopmans identifies as the current period of the *juridification* or legalization of social problems, of which surveillance is but one. Koopmans argues that the current period is further characterized by "*juridicialisation*, a process in which courts, not city councils, ministers or administrative agencies, are gaining importance in the protection of human rights."[21] According to his analysis, the political effects of juridification and juridicialisation are apparent in the move away from policy as a way of solving or managing social problems and the simultaneous move toward individual rights and, consequently, the law. Koopmans predicts that "informational privacy in the future will probably be assured by less emphasis on regulation and administrative systems of surveillance, and by more emphasis on individual rights and protection by the courts. These tendencies may constitute the new dialectics of privacy, perhaps

---

[19] Koopmans, pp. 48
[20] Ibid.
[21] Ibid., pp. 49

those of the 21st century."[22] The emphasis on individual rights is clearly reflected in Flaherty's table of privacy interests, and in the legalistic surveillance literature more generally.

The discourse of rights has come under criticism from a variety of sources, and it is certainly well beyond the scope of this paper to address these criticisms here in any systematic fashion.[23] There are, however, certain points that are particularly salient in the context of the right of privacy and the problem of surveillance more generally. In the first instance, the veil of ignorance and other myths like it do not capture the reality of surveillance, which most often does not operate on anything that even approaches a level playing field. There is certainly a politics of the watcher and the watched, and this politics has been effectively erased by the discourse on privacy. This is perhaps especially true in the context of employee e-mail monitoring, where the employee clearly does not enjoy the same position of power as the employer or the system administrator. The failure of privacy discourse to address these inequalities has the effect of rendering invisible the disciplinary functions of surveillance. So while the disciplinary effects of surveillance are clearly significant, they cannot be addressed through recourse to the concept of privacy.

The inability of the legal discourse around surveillance to get at issues of discipline highlights a further shortcoming of that approach. The characterization of the bearers of privacy rights as rational, mutually disinterested, self-identical subjects prevents legal theorists from considering the ways in which subjects are effected, and perhaps changed, by surveillance. The only effect which is taken to be significant, in this view, is the loss of privacy associated with surveillance. As a

---

[22] Ibid., pp. 51.

[23] The literature in this area is vast. I would, however, direct the reader to, for example, Susan Moller Okin, Justice, Gender and the Family. (New York: Basic Books, 1989); Michael Sandel, Liberalism and the Limits of Justice. (New York: Basic Books, 1983); Robert Nozick, Anarchy, State and Utopia. (New York: Basic Books, 1974); Michel L. Walzer, Spheres of Justice (New York: Basic Books, 1983); Alasdair MacIntyre, After Virtue (Nortre Dame: University of Notre Dame Press, 1988) and Whose Justice? Which Rationality? (New York: Cambridge University Press, 1988); Charles Taylor, "Cross Purposes: The Liberal Communitarian Debate" in Liberlism and the Moral Life, ed. Nancy Rosenblum (Cambridge: Harvard University Press, 1989); Virginia Held "Mothering versus Contract" in Beyond Self Interest. Jane J. Mansbridge, ed. (Chicago: Chicago University Press, 1990); Rita Manning, Speaking from the Heart: A Feminist Perspective on Ethics.

result, the legal approach structures resistance to surveillance in ways that fail to recognize or address questions about surveillance and subjectivity. But some of the aims of surveillance are clearly disciplinary in nature. Gandy's panoptic sort, for example, does not simply watch and record buying habits, it also motivates and manipulates changes in those habits.[24] Thus it has a role in *constituting* subjects as particular kinds of consumers.

The rights-based approach to surveillance, then, does not and cannot provide the necessary tools for recognizing, accounting for, or explaining the social effects of surveillance. So in effect, it does not confront surveillance on its own terms, but rather limits the problematization of surveillance to those aspects that relate to the infringement of privacy. Surveillance, however, is most often not carried out with the intention of invading privacy for its own sake; the invasion of privacy is, in many cases, simply a side-effect or a "useful by-product" of surveillance.[25] Furthermore, the problematization of surveillance on the grounds of the invasion of privacy has tended to privilege the individual in a way that makes it difficult to see the larger, cumulative effects of surveillance upon society. This has significantly hindered the ability of the legal discourse to recognize and account for the larger patterns of systematic surveillance which are characteristic of surveillance societies as we near the end of the twentieth century.

While the legalistic theories of surveillance clearly have their shortcomings, they have been instrumental in providing whatever protection against surveillance we have enjoyed until now. Privacy legislation has formalized and regularized individual entitlements to privacy and, in doing so, has sought to strike an acceptable societal balance between secrecy and openness, at least in relation to government data collection activities. Most privacy legislation is based on some variation of fair information principles (FIPs), also called privacy principles. While these principles tend to vary to reflect particular circumstances, Flaherty's table of Data Protection

---

[24] Gandy, op. cit., pp. 62.

[25] Jenkins, op. cit., pp. 14. Jenkins is referring here to cases where certain kinds of surveillance practices have provided information useful in apprehending criminals, even though the reasons behind the surveillance have nothing to do with crime control or law enforcement. In these cases, the invasion of personal privacy and the use of this information for law enforcement really is just a "useful by-product" of the surveillance. See Jenkins' article for a fuller explanation and examples.

Principles and Practices for Government Personal Information Systems, reproduced below, is a good example of fair information principles being put to use. According to Flaherty, such systems should conform to the following:

1. The principles of publicity and transparency (openness) concerning government personal information systems (no secret data banks).
2. The principles of necessity and relevance governing the collection and storage of personal information.
3. The principle of reducing the collection, use, and storage of personal information to the maximum extent possible.
4. The principle of finality (the purpose and ultimate administrative uses for personal information must be established in advance).
5. The principle of establishing and requiring responsible keepers for personal information systems.
6. The principle of controlling linkages, transfers, and interconnections involving personal information.
7. The principle of requiring informed consent for the collection of personal information.
8. The principle of requiring accuracy and completeness in personal information systems.
9. The principle of data trespass, including civil and criminal penalties for unlawful abuses of personal information.
10. The requirement of special rules for protecting sensitive personal information.
11. The right of access to, and correction of, personal information.
12. The right to be forgotten, including the ultimate anonymization or destruction of almost all personal information.[26]

Flaherty's table captures the essence of fair information principles, which is the idea that personal information should be collected and used only for particular, previously-identified reasons, and that it should not be shared without the consent of the data subject.[27] Fair information principles serve an important evaluative function in that they provide a mechanism for distinguishing between surveillance that is "fair" and that which is excessive. The provision of such a mechanism is based on the presumption that a certain amount of surveillance is inevitable, or possibly even desirable, and that the problem, when there is one, is one of imbalance.

---

[26] Flaherty, Protecting Privacy in Surveillance Societies. pp. 380.

[27] For other examples of fair information principles, see Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder flows of Personal Data. Paris: OECD, 1981 and Colin J. Bennett, Implementing Privacy Codes of Practice. Etobicoke: Canadian Standards Association, 1995.

Although FIPs can be used as a standard against which to measure the particular contents of any given data base, or to evaluate the information practices of various bodies, their utility as an evaluative tool must not be overstated. Their effectiveness is significantly hampered by the fact that FIPs provide their own internal standards of fairness. The principles of limitation and finality require that organizations generally only use or disclose information they have collected for the purposes for which is was collected, or for "consistent uses." In effect, this "means that organizations cannot change their minds about the uses they (or others) wish to make of personal information, after the event of collection."[28] But this limitation will clearly only have an impact where organizations have been required to define, clearly and narrowly, their purposes in collecting the information in the first place. At present, there is generally nothing to stop organizations from delimiting a wide variety of uses for the information and maintaining that the collection is still open and fair. FIPs, then, provide no limit to the kind of information that can be collected. "By these criteria, organizations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them, and accumulate ever more power over their lives."[29] Thus, while FIPs have been an important part of efforts to protect privacy in surveillance societies, the protection they have afforded has arguably provided a false sense of security.

On the whole, then, legalistic understandings of surveillance, while they have been extremely influential in framing debates and identifying the issues, have been so concerned with privacy and rights that they have overlooked the larger social issues at stake in these debates. As a result, the strategies of resistance which have emerged from legal framings of the problem of surveillance have not addressed the relationships between surveillance practices, or between surveillance and power.

---

[28] Graham Greenleaf, *In cyberspace, everyone will be anonymous for 15 minutes (A vision of privacy in the 21st century),* presented at Visions for Privacy in the 21st Century: A Search for Solutions (conference) Victoria, British Columbia, May 9-11, 1996, pp. 9.
[29] Rule et al., op. cit., pp. 8.

Anonymity and Data Security: A Technological Reading of Surveillance

Proponents of the technological approach to surveillance have played an increasingly important role in framing debates about e-mail security and privacy. In the context of these debates, the technological position has been articulated primarily by Cypherpunks[30] and crypto rebels, who have been very much involved in the development and dissemination of privacy-enhancing electronic technologies such as cryptography, anonymous mail forwarding systems, digital signatures, and electronic money. Their vision of electronic privacy is a radical one -- they "hope for a world where an individual's informational footprints...can be traced only if the individual involved chooses to reveal them; a world where coherent messages shoot around the globe by network and microwave, but intruders and feds trying to pluck them out of the vapor find only gibberish; a world where they tools of prying are transformed into the instruments of privacy."[31] Cypherpunks work from the bottom up, and maintain that "[w]e cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence...We must defend our own privacy if we expect to have any."[32] Their commitment to securing privacy protection from the bottom up is reflected not only in their political activism and lobbying efforts, and also in their involvement in writing privacy-enhancing software and disseminating it widely and, most often, for free.

In the United States, such activities have occurred in a politically charged and hotly contested atmosphere. The National Security Agency (NSA) has traditionally held a monopoly on cryptographic technologies and their development. This

---

[30] According to Stephen Levy, Cypherpunks are "a loose federation of computer hackers, hardware engineers and high-tech rabble-rousers." *The Cypherpunks vs. Uncle Sam*, in Lance Hoffman, ed. Building in Big Brother: The Cryptographic Policy Debate. (New York: Springer-Verlag, 1995) pp. 266. But, as Levy notes elsewhere, "it would be wrong to think of Cypherpunks as a formal group. It's more a gathering of those who share a predilection for codes, a passion for privacy, and the gumption to do something about it." Levy, *Crypto Rebels*. Just as one would expect, Cypherpunks have a strong presence on the network. Some good resources include: the Cypherpunks archives at http://ftp.csua/berkeley.edu/pub/cypherpunks/Home.html; and the Electronic Frontier Foundation (EFF) Archives at http://www.eff.org/pub/Privacy. Another excellent site is Matt Tomlinson's Cypherpunk's Topics at http://weber.u.washington.edu/~phantom/cpunk/index.html.

[31] Stephen Levy, Crypto Rebels, Wired. Electronic document available at http://www.eff.org/pub/Privacy/crypto_rebels.article (unpaginated). Also appeared in printed form in Wired magazine, issue 1.2.

[32] Eric Hughes, A Cypherpunk's Manifesto. Electronic document, available at http://weber.u.washington.edu/~phantom/cpunk/cpunk.manifesto

monopoly can be traced to the classification of cryptography as a weapon on the U.S. Munitions list. The NSA's monopoly was ensured by the Arms Regulation law, which controls the weapons found on that list. In 1975, the NSA's monopoly began to slip away. Whitfield Diffie, who was working in computers at Stanford, developed a new cryptographic system called public-key encryption. Diffie's system circumvented what he saw as the major flaw of earlier systems -- their reliance on top-down security systems where files were protected by user passwords which were accessible to system administrators. In these systems, the users' privacy depended largely on the will of the system administrators. As Diffie noted, this system was fundamentally weak: "You may have protected files, but if a subpoena was served to the system manager, it wouldn't do you any good...The administrators would sell you out, because they'd have no interest in going to jail."[33]

Existing encryption systems at that time were unwieldy and, because they used the same key to encrypt as to decipher messages, always involved the problem of how the key should be communicated to the receiver. This either required that the key be communicated over insecure channels, making it vulnerable to interception, or that central key repositories be established, thereby placing the final responsibility for privacy protection outside the hands of users. Diffie and collaborator, Martin Hellman, developed the public-key system to address these flaws. The principle behind their system was a simple one: each user had both a public and a private key. The public key would be widely distributed while the private key would be kept strictly secret. A message encoded with one key could be decoded with the other. So, for example, I could send you a message encrypted with your public key which you would then decode using your private key. If we were involved in a transaction where authentication was important, I could encrypt my message with my private key (since I would be the only one who knew that key, you could be sure that the message was really from me), and you could decipher it using my public key.

Diffie's public-key system was revolutionary, and by 1977 a set of algorithms that implemented the scheme, called RSA, had been developed. RSA provided stronger encryption than the government-approved Data Encryption Standard

---

[33] Levy, *Crypto Rebels*.

(DES), which was developed by the IBM research labs. DES is not a public key system, which means that the same key is used to encrypt and decrypt messages, and its key size is limited to 56 bits. By contrast, RSA can accommodate keys of any size, thereby providing greater security.[34] The RSA algorithms were patented and licensed to RSA Data Security, "whose corporate mission was to create privacy and authentication tools."[35] But Cypherpunks were not prepared to leave the protection of their privacy in the hands of a corporation, even a well-meaning one.[36]

Enter Phil Zimmermann, a political activist and computer programmer. When Zimmermann learned of public-key encryption, he became interested in finding a way to adapt it to personal computers using the RSA algorithms. Although he started working on his software in 1984, it was not ready for release until 1991. Around that time, Zimmermann heard about a proposed Senate bill that would ban cryptography, and quickly released his Pretty Good Privacy (PGP) software for free, "hoping it would spread so widely that the government could not suppress its use."[37] A friend of Zimmermann's posted it on the Internet, making it available for anyone in the world to download.

The government's interest was piqued; under U.S. export law cryptographic technologies are considered to be munitions -- a reflection of the NSA's former monopoly of those technologies. As such, strong encryption software like PGP cannot be exported outside the U.S. without a license, even though strong encryption is already available in many other countries. This policy has had a tremendous impact on the availability of strong encryption for software buyers in the U.S.. While "it is perfectly legal to build uncrackable crypto in products sold in the United States ... if companies grant strong privacy to their domestic users, the government will not let them ship those products to international customers, who often constitute half their revenues."[38] Since it neither practical nor cost-effective to

---

[34] The strength of encryption is measured by how hard the key is to crack, which is expressed in terms of bit length. The more bits or characters in a key, the more difficult it is to break the code. There were rumours that the NSA had forced IBM to make DES-encoding weak enough to permit the government to break the code if necessary for law enforcement purposes. These rumours were denied by the NSA. Reported in Levy, *Crypto Rebels*.

[35] Ibid.

[36] Ibid.

[37] Levy, *The Encryption Wars: Is Privacy Good or Bad?* Newsweek. April 24, 1995, pp. 56.

[38] Ibid., pp. 56.

ship two versions of the same software, U.S. companies must either provide weak encryption or no encryption at all. As a result, U.S. companies have lost sales to foreign competitors who do not have such restrictions. At the same time, they have not been able to provide domestic users with the protection afforded by strong encryption.

While the U.S. government stands behind its export policy, it has come under vehement attack from Cypherpunks and other civil libertarians. In this battle, Zimmermann has emerged as a hero. Although the U.S. government brought Zimmermann up on charges of violating export control legislation, those charges were later dropped. The battle, however, is far from over. Recognizing that strong encryption is now readily available to anyone who takes the time to download the software, the Clinton administration has attempted to stave off what the Cypherpunks affectionately call "crypto anarchy" with its Clipper and Clipper II schemes.[39] Essentially, the Clipper proposals involve a key escrow system which would provide a back door that would allow law enforcement and government security agencies to override people's private keys to gain access to encrypted electronic files. "The technology is based on a tamper-resistant chip that implements an NSA-designed encryption algorithm called SKIPJACK, together with a method that allows all communications encrypted with the chip, regardless of what session key is used or how it is selected, to be decrypted through a special chip unique key and a special Law Enforcement Access Field (LEAF) transmitted with the encrypted communications."[40] The system is designed to become the government standard for "sensitive but unclassified telecommunications, including voice, fax, and data transmitted on circuit-switched systems at rates up to 14.4 kbps or which use basic-rate ISDN or similar wireless service."[41]

---

[39] For a good overview of the Clipper wars, see Hoffman, ed., Building in Big Brother. Excellent resources are also available on the Web, most notably through the Electronic Frontier Foundation (EFF) at http://www.eff.org/pub/Privacy, and also through Wired Magazine's Home Page at http://www.hotwired.com/frontdoor/. Crypto anarchy refers to the crypto rebel vision of a future where strong encryption is widely available and put to use without government interference or control.

[40] Dorothy E. Denning, *The U.S. Key Escrow Encryption Technology,* in Hoffman, ed. Building in Big Brother. pp. 111.

[41] Ibid., pp. 112.

While the SKIPJACK algorithm has an 80-bit key, which provides what is generally considered to be strong encryption, critics of the Clipper scheme maintain that the strength of the encryption is irrelevant when law enforcement authorities have access to the code.[42] But the Clinton administration argues the key escrow system, which would be voluntary under present proposals, serves an important function in terms of the law and order agenda. The NSA and the FBI are apparently concerned that terrorists and criminals will use strong encryption to communicate with one another and to shield their activities. The key escrow system would "help law enforcement agencies thwart criminals and terrorists who might use advanced telecommunications to commit crimes."[43]

The original Clipper proposal fired off a fury of controversy, and was finally defeated largely because of the vigorous involvement of the crypto community. The administration came back with the Clipper II scheme, which retains most of the provisions of the original proposal. Clipper II is still being debated, and there is no doubt that the stakes are high. The crypto community sees the Clipper proposals as a last-ditch effort on the part of the American government to seize control of cyberspace. And while concerns about criminal and terrorist activities may well be valid, they are not enough to "halt the spread of crypto anarchy. Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures."[44]

---

[42] It is unclear whether such access would have the same restrictions that currently control wiretapping. While most souses suggest that this would, indeed, be the case, Meeks notes that Assistant U.S. Attorney Kent Walker "seemed to be lobbing for the opposite. Giving the Fed the ability to listen in first and give justification later amounts to "no big difference," he said. Besides, "it would save time and money." And Walker promised that law enforcement would only use this power against evil, never abusing it." Meeks, *The End of Privacy*, unpaginated.

[43] Vice President Gore, as quoted in Brock N. Meeks, *The End of Privacy* in Wired. Early release electronic document, available through Wired Online/Hotwired, http://www.hotwired.com/frontdoor. Final draft appeared in printed form in Wired magazine, issue 2.04, April 1994.

[44] Timothy May, The Crypto Anarchist Manifesto. Electronic document, available at http://weber.u.washington.edu/~phantom/cpunk/crypto.anarch.manifesto.

For Cypherpunks and crypto rebels, the availability of strong encryption is a civil liberties issue. The government's proposed key escrow system, they argue, is akin to asking people to provide a copy of their house keys to law enforcement authorities. And while, for the moment, the proposed Clipper scheme would be optional, there is guarantee that it would stay that way. Furthermore, software companies that want to do business with the U.S. government would be required to serve up "crypto lite," making weak encryption the defacto standard.[45] This tendency could be reinforced by the use of the existing export laws to require Clipper chips in computers shipped out of the United States.[46]

In some ways, getting strong privacy protection is just the tip of the iceberg in terms of the Cypherpunk agenda. Their commitment to strong encryption is about more than just privacy, though privacy is certainly a major concern. It is part of a larger vision, where the value of strong encryption "will be to provide anonymity, the right most threatened by a fully digitized society."[47] While Cypherpunks assert the right to anonymity again and again, there seems to little interest in talking about just what kind of claim is being made. When it is spoken of, the right to be anonymous seems to be related to, but also distinct from, the right of privacy. In the Cypherpunk literature, the rhetoric of privacy is largely one of inarticulated origins and sweeping statements; Hughes opens his Cypherpunk Manifesto with the statement that "[p]rivacy is necessary for an open society in the electronic age."[48] This may well be so, but Hughes does not articulate how a *right* of privacy follows from a need for it. Instead, he makes vague appeals to cherished American political ideals, warning that "for privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good."[49]

While the technologically-oriented literature on digital surveillance seems only peripherally interested in privacy as a philosophical problem, the practical aspects of privacy protection and the preservation of anonymity have constituted

---

[45] This term is borrowed from Levy, *The Cypherpunks vs. Uncle Sam*, pp. 275.
[46] John Markoff, *Ideas and Trends: Cyberspace Under Lock and Key*. Electronic document from cypherpunks-list #10116. Originally appeared in New York Times. Sunday, February 13, 1994.
[47] Levy, *Crypto Rebels*.
[48] Hughes, op. cit.
[49] Ibid.

that literature's major preoccupations. A further preoccupation has centred around issues of communications privacy and data security. The concern is that, in an increasingly digitized society such as ours, digital trails -- "health records, phone bills, credit histories, arrest records and electronic mail" [50] -- can be used to compile extremely detailed individual profiles. The existence of these profiles, and the ease with which they can be both generated and disseminated seriously undermines our fundamental right to anonymity. To get around this problem, they argue, "we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction."[51]

To that end, Cypherpunks and others have been very active in developing technologies that limit the amount of data necessary to engage in transactions. Perhaps one of the most influential figures in this field has been David Chaum. Chaum's company, Digicash, has been at the forefront of developments in anonymous digital money systems. In an 1992 which has become a classic in the field, Chaum outlines what he sees as the primary issue in digital cash systems: the need to prevent fraud while protecting the privacy of individuals involved in transactions. Chaum notes that "organizations link records from different sources for their own protection. Certainly it is in the interest of a bank looking at a loan application to know that John Doe has defaulted on four similar loans in the past two years. The bank's possession of that information also helps its other customers, to whom the bank passes on the cost of bad loans."[52]

The linking of information from a variety of sources is made possible by the use of particular identifiers, such as social insurance numbers. The use of such identifiers, argues Chaum, "perforce trades off security against individual liberties."[53] In order to redress this imbalance, Chaum and his colleagues from the Cryptography Group at the Dutch Center for Mathematics and Computer Science in Amsterdam developed techniques that "avoid the possibility of fraud while maintaining the privacy of those who use them."[54] Chaum describes these techniques as follows:

---

[50] Levy, *Crypto Rebels*.
[51] Hughes, op. cit.
[52] David Chaum, *Achieving Electronic Privacy*, Scientific American. August 1992, pp. 86.
[53] Ibid., pp. 96
[54] Ibid.

> In our system, people would in effect give a different (but definitively verifiable) pseudonym to every organization they do business with and so make dossiers impossible. They could pay for goods in untraceable electronic cash or present digital credentials that serve the function of a banking passbook, driver's license, or voter registration card without revealing their identity. At the same time, organizations would benefit from increased security and lower record-keeping costs.

The exact technical specifications of Chaum's system are not important for my purposes here.[55] What *is* important is how Chaum situates his own project. His system is a response to what he perceives to be the relevant interests in electronic transactions: the interest of businesses in protecting themselves against fraud and the interest of individuals in protecting the privacy of their personal information. But Chaum's understanding of the interests of business in transactional information is somewhat thin. He fails to recognize that, in the context of emerging information markets, the data that are generated by transactions are valuable commodities in themselves.[56] This is a significant consideration, for clearly the widespread implementation of anonymous transaction systems will require the cooperation and support of business and government. What is not clear, however, is why businesses would grant such cooperation when Chaum's scheme would seriously impede their efforts at targeted marketing and cost them in lost revenues from the sale and/or rental of lists. While it is certainly true that an anonymous sale is better than no sale at all, those sales which generate transactional data are doubly valuable because they contribute to future sales by providing the basis for targeted marketing.

Chaum's failure to address these issues is typical of the Cypherpunk literature. Yet this failure is a somewhat surprising one given that one of the driving forces behind the fight for strong encryption and other privacy-enhancing technologies has been the belief that, in the future, more and more business will be conducted electronically. But while business may well be prepared to stand behind strong encryption, which will arguably give consumers the confidence to engage in electronic transactions, it does not follow that they will stand behind the technologies

---

[55] At any rate, Chaum's explanation of the system in his Scientific American article borders on the incomprehensible in places. For a more accessible overview of some of the technologies at work here, see Ann Cavoukian, Who Knows: Safeguarding Your Privacy in a Networked World. (Toronto: Random House, 1995) pp. 131-157.

[56] The most notable recent work on this theme is Gandy's The Panoptic Sort.

of anonymity being championed by Cypherpunks and crypto rebels. Still, many members of the crypto community seem to think that crypto anarchy is virtually inevitable. Timothy May, author of the Crypto Anarchist Manifesto of 1988, predicts that developments in personal computers in "the next ten years will bring enough additional speed to make the ideas [of crypto anarchy] economically feasible and virtually unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-purpose MIPS personal computers, and encryption chips now under development will be some of the enabling technologies."[57]

Now, eight years after May wrote those words, the technologies of crypto anarchy are, indeed, becoming increasingly available. But the fact that these technologies exist does not ensure that they will prevail, despite May's technological determinism. And if the battle over the Clipper schemes is any indication, the Cypherpunks are clearly in for a fight. The apparent naiveté of the crypto community with respect to the incentives for business to collect transactional data may well hinder them in this fight.

A Sociology of Surveillance: Models of Social Control

While Cypherpunks and crypto rebels exhibit only a limited sensitivity to the social context in which contemporary surveillance practices are emerging, sociologists of surveillance have been almost entirely preoccupied with the interplay of surveillance and established or emerging social orders. In contemplating this relationship, the sociological literature has addressed such issues as the effects of surveillance on the link between labour and capital, and the ways in which surveillance practices work to reinforce social and economic hierarchies based on race, class, and gender. For my purposes here, the themes which have been particularly significant in the sociological literature on surveillance are those which touch upon the relationship between surveillance and social order. Here Foucault's work on panopticism as a form of discipline has been extremely influential.

Oscar Gandy is among those theorists who have been very much influenced by the metaphor of the Panopticon. Gandy has written extensively on the use of

[57] Levy, *Crypto Rebels*.

surveillance as a tool of classification in the context of consumer culture. Information is collected from a variety of sources in order to compile consumer profiles which permit marketers to categorize consumers in a process that Gandy calls the 'panoptic sort.' Like the Cypherpunks and crypto rebels, Gandy is concerned by the ease with which detailed electronic profiles can be generated. But his concern is less with preserving a right to anonymity than with understanding the social effects of the ways in which these profiles are created and used. For Gandy, the panoptic sort is "a kind of high-tech cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value."[58] It increases the ability of organized interests to "identify, isolate, and communicate differently with individuals in order to increase their influence over how consumers make selections."[59] This ability, argues Gandy, serves to further entrench pre-existing social hierarchies based on the ability to consume, and packages those who are at the margins of consumer culture as an underclass of "damaged goods to be discarded or sold at bargain prices to scavengers in the marketplace."[60]

The panoptic sort, then, is essentially a vehicle of discrimination which is fueled by the personal information collected and extrapolated from various sources and combined with environmental information. This information occasionally comes from government data banks and census data, but more often from other sources, including applications for services such as insurance and utilities, surveys and samples, contest entries, credit card records, educational information, newspaper and magazine subscriptions, real estate information, legal records, and rental agreements of various kinds. The panoptic sort is the technological *process* through which this information comes to be collated, analyzed, and used to differentiate between and manipulate or "manage" market segments. This process is guided by instrumental rationality and has stages and "component parts that vary in importance, depending on the purposes and interests of the controller."[61] Gandy

---

[58] Ibid., pp. 1.
[59] Ibid., pp. 2.
[60] Ibid.
[61] Ibid., pp. 80.

lists these stages as identification, classification, prediction, prevention and avoidance of risk, and allocation of life chances.[62]

The first stage, identification, is essential to the functioning of the panoptic sort, for it is through identification that individuals are able to negotiate the bureaucratic maze that characterizes surveillance societies. James Rule has suggested that there are two types of identification: the documentary tokens that we carry around with us, such as driver's licenses or health care cards, and the data stored in the files held by the organizations that issue these tokens or require their production for the completion of a transaction. These two types of identification work in conjunction with one another to fulfill the socially and bureaucratically significant function of generating certainty about people. Rule argues that it is based on this certainty that organizations are able to "discriminate in their treatment of individuals."[63]

The second stage of the panoptic sort involves the segmentation and classification of individuals into groups. Classification is essentially a mechanism of control, "driven by the purposes or interests of the actors who seek to take advantage of knowledge regarding the factors that produce or underlie the similarities or differences between people."[64] The classification schemes of the panoptic sort reflect at least two instances of the functioning of power. In the first instance, the organizations behind the panoptic sort determine the parameters of the relevant market segments. In doing so, they effectively determine which similarities and differences will be socially significant and which will be marginalized or rendered invisible. In a culture of consumption, difference comes to be defined to a large degree through the erection of boundaries between market segments. Thus it is tremendously significant that these boundaries should reflect the purposes and interests of the powerful organized interests behind the "all-seeing eye of the difference machine."[65]

The functioning of power is also apparent, in the second instance, in the process by which individuals are classified as belonging to one market segment or

---

[62] Ibid.
[63] James B. Rule et al., *Documentary Identification and Mass Surveillance in the United States*, pp. 222 - 234.
[64] Gandy, pp. 82.
[65] Ibid., pp. 2.

another. As Gandy notes, "classification generally involves some form of measurement or weighing."[66] In the context of the panoptic sort, this has entailed the evaluation of an individual's ranking within a hierarchy based on market values. One's ranking in this schema reflects social status and economic power or potential, and is consequently of tremendous social significance. Classification, both generally and within the specific context of the panoptic sort, determines how particular groups are framed in a variety of circumstances.[67] Thus labels have become highly contested political sites.[68] In particular, the recognition of the political effects of labeling has made individuals and groups increasingly interested in claiming for themselves the power to classify. The tension between labels that are chosen and those that are attributed, for example, "plays itself out in the continually changing category schemes for the census and other surveys that take note of racial and ethnic group membership."[69]

The panoptic sort is clearly and profoundly invested in maintaining the present system whereby labels are externally imposed upon consumers. Part of this investment reflects the importance of the panoptic sort as an instrument of prediction. According to the logic of the panoptic sort, once individuals have been identified and assigned to a particular category or market segment their behaviour can be predicted based on the norms for that group. Gandy's analysis of this

---

[66] Ibid., pp. 83.

[67] Thus, as Mary Douglas argues, the process of labeling can lead to very different approaches to public policy, as in the use of the label "vagrant" rather than "homeless." See Mary Tew Douglas, How Institutions Think (New York: Syracuse University Press, 1986), pp. 58.

[68] Identity politics have, in some sense, been a politics of classification, though they have generally served to reinforce the rigidity of categories rather than to open them up to scrutiny. The rhetoric of identity politics has tended to focus on a fixed hierarchy of oppressions along particular axes, such as race, sexuality, and gender. The difficulties associated with such a stance been a recurrent theme in a number of different literatures. See, for example, Kobena Mercer, *Welcome to the Jungle: Identity and Diversity in Postmodern Politics,* Identity: Community, Culture, Difference. Jonathan Rutherford, ed. (London: Lawrence and Wishart, 1990); Judith Butler and Joan W. Scott, eds. Feminists Theorize the Political. (New York and London: Routledge, 1992); Chandra Talpade Mohanty, *Cartographies of Struggle: Third World Women and the Politics of Feminism,* Third World Women and the Politics of Feminism. Chandra Talpade Mohanty, Ann Russo and Lourdes Torres, eds. (Bloomington and Indianapolis: Indiana University Press, 1991); Kathy Ferguson, The Man Question: Visions of Subjectivity in Feminist Theory. (Berkeley: University of California Press, 1993), especially chapter 6.

[69] Gandy, op. cit., pp. 82.

process leads him to suggest that the panoptic sort is, at its foundation, a technology of risk avoidance. As such, it is concerned with "deselecting rather than including and ... is based on probabilistic rather than exact predictions."[70] According to Gandy, risk avoidance strategies contribute to an increasingly actuarial model of social control which functions based on "probability, opportunity reduction, and loss prevention."[71] These calculations make it possible to anticipate and minimize loss by reducing or avoiding contact with individuals or groups who represent avoidable risk. In order for this scheme to work, however, the risk-generating behavior or behaviors must be of a repetitive nature. The functioning of the panoptic sort also depends, in part, on the "similarities in the circumstances as well as a finite limitation on the number of relevant variables one can include in the predictive model."[72] Thus, Gandy notes that

> insurance based techniques of control are largely mass produced and data dependent, and, thus, they require a level of routinization that has not been typical of social control in the past. Information that is used to screen, sort, classify, and exclude needs to be standard, and clearly defined so that it can be quickly evaluated.[73]

This level of routinization is apparent, for example, in the credit and financial services industries. Since consumer credit operates with very little collateral, the costs of defaulting are very high for credit providers. "Thus the art and science of credit management lie in determining, in advance, who will pay and who will not, and in screening credit applicants accordingly."[74] Risk is minimized not by coercing those who misbehave, but rather by limiting their participation in circumstances where they might be tempted to misbehave. The risk avoidance model of social control, then, is based on the principle of *exclusion* rather than *coercion* and excludes "would-be delinquents from the opportunity to disobey the rules."[75]

While risk assessment and avoidance have certainly been important functions of the panoptic sort, its principal function has unquestionably been to serve

---

[70] Ibid., pp. 84-85.
[71] Ibid., pp. 85.
[72] Ibid.
[73] Nancy Reichman, *Managing crime risks: Toward an insurance based model of social control*, Research in Law, Deviance and Social Control 8 (1986): 151-172, as quoted in Gandy, pp. 85.
[74] Rule, Private Lives and Public Surveillance, pp. 178.
[75] Ibid., pp. 179.

as an instrument of consumer targeting. For once poor risks have been eliminated, attention can be focused on those market segments that offer the highest probability of success. This function of the panoptic sort has evolved from earlier forms of consumer targeting which were based on the neighborhood characteristics which could be gleaned from census data. Later, targeting techniques were refined using technologies such as geocoding, where geographical codes are assigned to records of events or other descriptive data. At its height, geodemographic clustering linked "extensive socioeconomic data to postal zip codes, which had been classified into one of forty different kinds of neighborhood types."[76] Such techniques were further developed and refined with the increased availability of income and demographic information, which allow for more detailed profiling. The resulting ability to target individuals and groups with unprecedented precision has been a great boon to marketers and political strategists.

In practice, commercial and political targeting "moves back and forth from high levels of aggregation to the identification of specific individuals based on an assessment of how they will respond to a particular issue, opportunity, or challenge."[77] Thus the panoptic sort is also, in part, the mechanism by which the flow of information to particular individuals or groups is determined. Those who are labeled as being members of the least desirable market segments receive the smallest amount of information and the fewest opportunities to consume. Those in the most desirable segments, by contrast, are rewarded with more and more opportunities to consume.

The uneven flow of information which is facilitated by the functioning of the panoptic sort, argues Gandy, is fundamentally antidemocratic because its aim is nothing less than the "rationalization and control of human existence."[78] The panoptic sort is, in Gandy's terms, a technology of control, developed during the "control revolution in late capitalism," and is "incompatible, mutually inconsistent, contradictory, and antagonistic to the notion of free acting, fully informed rational producers and consumers."[79]

---

[76] Gandy, pp. 87.
[77] Ibid., pp. 89.
[78] Ibid., pp. 227.
[79] Ibid.

In its allocation of life chances, the panoptic sort rewards those who give up their personal information (whether they do so consciously or not), especially when that information leads them to be classified as "good" consumers. Resistance in the form of refusing to feed the machine with personal information is practically futile, since "the power that the individual is able to exercise over the organization when she withholds personal information is almost always insignificant in comparison with the power brought to bear when the organization chooses to withhold goods or services unless the information is provided."[80]

Gandy's work has been an important contribution to surveillance theory in so far as it highlights the political effects as well as the political context of surveillance. Thus even if one finds Gandy's claims to be occasionally exaggerated or insufficiently substantiated, the utility of his approach is, in my opinion, undeniable. More particularly, Gandy's text provides an excellent synthesis of a number of the approaches and traditions which have figured prominently in surveillance discourse. Among his influences are Marx, Weber, Foucault, and Giddens. These varied influences lend to Gandy's analysis a richness and depth which is rare in this literature.

Gandy's analysis leads him to conclude that the panoptic sort is fundamentally and intrinsically antidemocratic. As such, he argues, it cannot be changed or improved upon in ways that would transform it into a more egalitarian and democratic technology. Gandy's position here is similar to Gary Marx's. Marx sees in the expansion of surveillance in general, and of electronic surveillance in particular, the emergence of a "maximum security society." The positions articulated by Gandy and Marx are fairly common within the literature on surveillance. In that literature, surveillance has most often been portrayed as negative.

Some other theorists, however, have taken a different view, seeing nothing intrinsic about the ill effects of modern surveillance practices. Indeed, they argue that some modern surveillance practices provide, or could potentially provide, us with desirable social goods. David Lyon, for example, has taken this position. In contrast to Gandy, he characterizes the relationship between surveillance and social power as being a generally benign and subtle one, and argues that

---

[80] Ibid., pp. 19.

> [f]rom the point of view of the customer, new opportunities and benefits seem to abound with the advent of new technologies harnessed to spending...Consumer surveillance...is of a piece with designer goods, customized services, and other advances that take us beyond the world of standardized, uniform products and accompanying limits on consumer choice. Its enabling capacity seems unquestionably desirable.[81]

Lyon's focus on the benefits associated with consumer surveillance and targeting is in keeping with his view, expressed in more general terms, that surveillance *does* have a place in "the good society." In his sketch of the historical foundations and development of modern surveillance practices, Lyon plays up the theme of surveillance as a site of duality, as both force and counter-force, captor and liberator. While much of the discourse around surveillance, including Gandy's work, is framed around themes of invasion, capture, or loss, Lyon argues that surveillance has also functioned as a site of empowerment, dignity, and opportunity. In his discussion of the expanding administrative functions of the modern nation-state, for example, surveillance emerges not simply as a strategy of social control, but also as a vehicle of social participation. Historically, record-keeping became an increasingly important function of the nation-state as it took charge of providing various services and administering certain rights and duties. The extension of the franchise, for example, required the compilation of lists of eligible voters, just as the collection of taxes requires detailed personal and financial information about taxpayers. Thus way, the rights and benefits that are provided and safeguarded through the mechanisms of statehood also function to expand and entrench the state's surveillance function.

Lyon uses the notion that surveillance has a dual character, spelling "control *and* care, proscription *and* protection," as the basis for much of his critique of contemporary surveillance theory. In his view, surveillance theory has tended to overemphasize the negative aspects of surveillance, constructing surveillance as a site of "control, constraint, the probing eye, unfreedom."[82] In doing so, argues Lyon, surveillance theory has given itself over to paranoia. In order to remedy this situation, Lyon calls for a rethinking of how we approach surveillance in terms of

---

[81] Lyon, The Electronic Eye. pp. 140.
[82] Ibid., pp. 222.

understanding its historical context and development, as well as its location in a good society. By thinking through and articulating a conception of the good society, and the role that surveillance might play in such a society, surveillance theory can become, in Lyon's terms, "constructively critical."[83]

The problem for Lyon, then, is how to determine what the good society looks like and what its attributes are or might be.[84] In this task Lyon finds guidance in Saint Augustine's "other city." There social participation is based on a pre-existing, essential human solidarity and "personhood is understood not as the self-possessing individualism attacked by Augustine -- and which flourishes within privacy discourse today -- but as the *imago dei*, which again accents solidarity, dignity and responsibility."[85] From Augustine's other city, Lyon takes the values of participation, personhood, and purpose. He then attempts to apply those values in his thinking about surveillance and, more particularly, in his attempts to situate surveillance as a feature of the good society. In doing so, Lyon seeks to sidestep the obsessions with privacy and pessimism that he feels have characterized surveillance theory, and to instead make "genuine progress."[86]

Ultimately, Lyon fails to be persuasive in this line of argumentation. While it may be true that surveillance literature has tended toward the paranoid or the pessimistic, Lyon's claim that surveillance has been empowering is somewhat flimsy. More specifically, those aspects of surveillance that Lyon is touting as being positive, such as political or social participation, can also be understood as part of the process through which surveillance is normalized and made palatable. The promise of a social benefit or a civil liberty in exchange for the provision of information ensures that there is ample incentive for self-reporting. If one wants to vote, in other words, one will provide the necessary information to be included on voters lists. In this way the smooth functioning of surveillance is assured, and information can be collected with a minimum expenditure of effort.

Similarly, Lyon's apparent enthusiasm for targeted appeals to consumers is based on his belief that such appeals give consumers greater choice and therefore

---

[83] Ibid.
[84] I use *the* good society in the singular here very pointedly. It is the phrase that Lyon uses, and I think that it betrays his own universalizing impulses.
[85] Ibid., pp. 222.
[86] Ibid., pp. 223.

greater freedom. His assessment of consumer surveillance, then, hinges on the question of whether surveillance enables or constrains consumption. In Lyon's analysis, the ability to consume is an important expression of one's freedom. The extent to which surveillance is a problem, then, is determined by whether it inhibits or enables the freedom to consume. Lyon's approach is profoundly flawed, however, because it does not permit a meaningful analysis of how consumption *itself* functions to discipline subjects. As a result, Lyon is somewhat insensitive to the ways in which consumer surveillance reproduces the social order by differentiating between the opportunities for consumptive freedom that are offered to various market segments.

Other theorists, including Gandy, have been far more sensitive to such issues. And overall, there is no question that the sociologists are, in general, more sensitive to the complexity of the issues raised by surveillance in terms of its social and political effects. Neither the legal theorists nor the technologists have benefited from the richness of the sociological analysis, however. By the same token, the sociologists have been unable to articulate strategies of resistance that reflect their understanding of the effects of surveillance and, like the legal theorists and the technologists, often end up falling back on some version of privacy. Furthermore, some of the sociological literature displays a profound naiveté about the technologies at work.

Certainly a major part of the problem here has been that, within each literature, surveillance has been framed as a problem of law, technology, or society. In each instance, the approaches have been developed largely in isolation from one another. But there are clearly important insights to be gained from each of these literatures. The legal theorists, for example, have provided the best formalized protection against surveillance, and have sensitized law makers to the need to consider the privacy implications of new legislation. And while they have also provided the most thoughtful analysis of the concept of privacy, it remains a fundamentally flawed, though still useful, concept. Furthermore, the legal approach has tended to remain silent about the relationship between different surveillance practices. As a result, their understanding of the larger effects of surveillance is extremely thin.

The technologists, on the other hand, have provided the tools to ensure the best practical protection against surveillance, and have put those tools in the hands of individuals, granting them greater control over their own personal information. In this sense the technological approach to fighting surveillance has displayed a tremendous potential to empower individuals. But certain features of the technologist position reflect a failure to take into account the tremendous incentives that businesses have for collecting transactional data, and the relatively minor incentives for protecting privacy.

Finally, the sociologists have clearly provided the best theoretical analysis of both the larger effects of surveillance and the social context in which modern surveillance practices have emerged. In doing so, they have distinguished themselves from the other surveillance theorists by being able to account for larger patterns of surveillance. Furthermore, the sociological approach to surveillance addresses questions of discipline, which at least make it possible to consider issues of subjectivity, although few theorists have taken advantage of this possibility. And while the sociologists paint a very rich and complex portrait of surveillance, they seem paralyzed by its complexity, and have not been able to suggest strong measures to protect against surveillance.

There is clearly room for cross-fertilization in the three surveillance literatures. A recognition of the larger social effects of surveillance, for example, might lead legal theorists to demand stronger statutory protection against surveillance. By the same token, the technologists' position might be strengthened by a richer analysis of the concept of privacy, and of the context in which surveillance takes place. Finally, a consideration of the possibilities for individually empowering technologically-based resistance to surveillance might suggest to the sociologists that surveillance does not necessarily have to be a totalizing feature of modern life. Such cross-fertilization could only serve to enrich the present analysis of surveillance and to stimulate debate within the literatures.

A further shortcoming of the framing of surveillance as a problem of law, technology, or society has been the relative absence of a sustained *political* analysis of surveillance. Certainly some aspects of the debate around surveillance have been politicized, such as the Clipper campaign, but, by and large, there has been no

place in the literature for a serious and sustained consideration of how power functions in and through surveillance, and how the flow of this power might be effectively disrupted using counter-surveillance strategies. As a result, the literature on surveillance has also not been able to address such issues as the relationship between surveillance and subjectivity, or between subjectivity under surveillance and identity, among others. Those analysts who *have* been sensitive to political issues around surveillance have been few and far between, and include, most notably, Colin Bennett, Charles Raab, and Priscilla Regan. The work of such analysts contributes significantly to the beginnings of a *political* theory of surveillance.

So while there is clearly a need for dialogue between the various literatures on surveillance, there is also a need to expand the kinds of analyses that are being done. Thus, I would suggest, the literature on surveillance could well benefit from an incorporation of some of the themes and problematics of other literatures, especially those that have been preoccupied with questions of politics, identity, and subjectivity. In particular, I think that a consideration of some of the themes that have characterized post-structuralist literatures might lend a depth to the literature on surveillance which it presently does not have. In the next chapter, then, I look at what some of those themes have been, and consider how they might be fruitfully incorporated into the study of surveillance.

Chapter Four: Conclusion: (Be)Labouring the Subject.

In framing the problem of surveillance as one of law, technology, or society, current theories of surveillance have clearly rendered certain lines of inquiry either impossible or implausible. This becomes particularly evident when such theories are applied to a particular surveillance practice such as the problem of employee e-mail monitoring outlined in Chapter One. So I want to begin this chapter by considering the kinds of issues related to e-mail monitoring that are highlighted, explained, or accounted for by the legalistic, technological, and sociological literatures on surveillance. At the same time, and more importantly, I want to highlight those issues which are *not* highlighted, explained, or accounted for by these theories but are, rather, marginalized or erased.

From a legalistic point of view, the central problem in debates about the monitoring of employee e-mail has been the lack of clear parameters around the right of privacy with respect to electronic mail. According to the legal theorists, two things are needed in order to address this lack. First, the relationship between the right of privacy and other salient rights must be determined. Other salient rights in this case might include the right of employers to monitor the use of company resources, as well as their right to monitor employee productivity. Second, once an acceptable balance between competing rights in this instance has been achieved, this balance must be formalized through clear laws or policies which detail the extent of privacy that employees are entitled to. It is worth noting that, in all likelihood, this balance would favour the employer, since the employer can claim several rights in this instance while the employee can claim only one. Furthermore, it seems that, in practice, privacy rights can be surrendered by contractual agreement. Thus the degree to which employees can reasonably claim a general right of privacy in the workplace is delimited, at the outset, by the employment contract. When taken in conjunction with one another, it seems likely that these factors will tip the balance in favour of employer rights with respect to electronic mail privacy in the workplace.

Significantly, the way that the issue of surveillance is framed in the legal literature and, in particular, the emphasis on the concept of privacy, suggests that there are no interesting questions to be asked about the effects of surveillance upon

the subject. This message is conveyed in a number of ways, many of which are related to the fact that the legalistic literature builds its analysis of surveillance around a notion of subjects as unified, mutually disinterested, atomistic individuals who can be said to hold property in themselves. In this scheme, the concept of privacy becomes closely linked with the erection and patrolling of the vulnerable but nevertheless coherent and cohesive borders of the self which is distinguished from the other. While the construction of a right of privacy is, in some sense, designed to permit self-determination of these borders, the discourse of privacy does not really take seriously the possibility that subjects could be profoundly changed or disciplined through surveillance. In other words, the discourse of privacy does not entertain the idea that the boundaries between self and other might be so fluid as to be virtually meaningless in some circumstances. This is reflected in the championing of fair information principles, which do not adequately address issues of how subtle but insidious forms of power are exerted through surveillance, but rather seek to regularize and formalize the ways in which we are watched. As a result, the legalistic literature on surveillance cannot provide a framework through which to even contemplate the idea that surveillance might render the notion of self-determination meaningless by disciplining subjects at some fundamental or perhaps corporeal level.

The legalistic perspective on surveillance is further limited by its failure to duly consider the social context in which contemporary surveillance patterns have emerged. The kinds of social, political, and economic stimulants that have impacted on surveillance, and which were outlined in Chapter Two, are not considered in the legalistic analyses. Consequently, larger issues concerning the relationship between surveillance and social control are also not addressed under the rubric of privacy. This has had significant implications in terms of constructing surveillance as a particular kind of problem. The focus on privacy in the legalistic discourse suggests, as I noted above, that the real problem with surveillance is its limiting effect on self-determination, and not its role in maintaining pre-existing structures of power.

In terms of the specific case of employee e-mail monitoring, then, the legalistic discourse on surveillance focuses attention of a number of key factors: 1) the need to consider the relative weight of privacy and other salient rights, such as

the right of the employer to monitor the use of company resources, as well as to monitor the performance and/or productivity of company employees, 2) the need for policies which clearly state what the rules will be with regards to the use of company e-mail accounts, and 3) in more general terms, the loss of personal autonomy associated with surveillance. The legalistic discourse around surveillance does not, however, provide any mechanism for addressing the issue of subjectivity under surveillance, nor does it reflect any understanding of the role that surveillance plays in maintaining particular kinds of social control. Thus, for example, it does not provide any kind of framework for asking after the specific effects of employee e-mail monitoring, including such fundamental behavioural questions as whether employees use e-mail more or less frequently when they are aware of monitoring, or whether or not the contents of their messages change. Furthermore, the legalistic literature on surveillance does not provide an adequate vehicle for looking at how power is distributed in surveillance situations, and how that power is used to produce or reproduce social order. This seems especially significant in the context of the claim that e-mail is flattening corporate hierarchies, which are most probably being simultaneously reinforced by the monitoring of that e-mail.

A technological perspective on the practice of employee e-mail monitoring, by contrast, would call attention to issues of privacy related more directly to the design of e-mail systems. According to technologists, such systems are fundamentally flawed in that they lend themselves too easily to monitoring. Thus the best way to address the emerging problem of employee e-mail monitoring is to develop or use privacy-enhancing e-mail technologies. Such technologies might include, for example, encryption programs, where control of the keys is placed entirely in the hands of employees. Related problems pertaining to the security of electronic communications might also be addressed by encryption, and by other technologies such as digital signatures.

There are, of course, obvious problems with technological solutions to the surveillance problem. First, employers have already demonstrated a keen interest in monitoring both the flow and the content of employee e-mail. In order for privacy-enhancing technologies to be integrated into the workplace, employers would have to be convinced that their interest in preserving employee privacy is greater than

their interest in monitoring labour and labour processes. This seems unlikely, at best. Furthermore, workplace e-mail systems are provided by the employer for business purposes, and are provided using company resources. Thus the use of privacy-enhancing technologies such as encryption would have to initiated, or at least approved, by them. There seems to be no evidence to suggest that employers would find the need for employee privacy a compelling enough reason to give up their ability to monitor e-mail systems, even if they do not normally use that ability. This is underlined by the fact that privacy-enhancing technologies are increasingly available, and that there has been no movement on the part of employers to use such technologies for the purposes of protecting employee e-mail privacy.

The commitment on the part of technologists to privacy-enhancing technologies reflects, to a large extent, their assertion of anonymity and data security as primary values. The theme of anonymity is closely linked to the understanding of surveillance as a problem of unfreedom, which is to say that, in this literature, surveillance is seen as a problem to the extent that it inhibits freedom of communication or interferes with the right to control information flows about oneself. While the construction of this right is, in many ways, similar to the construction of the right of privacy in the legalistic discourse around surveillance, it is significantly amplified and extended by the concept of anonymity, which is distinguished from privacy in a number of ways. Perhaps the most important of these is that a right of anonymity precludes the formation of acceptable standards for surveillance, such as have been articulated in fair information principles, because any restriction of freedom through surveillance is deemed to be unacceptable. This reflects some recognition, on the part of Cypherpunks and crypto rebels at least, that surveillance takes place in a context of power, and that power functions *through* surveillance to reinforce existing power structures.

For the most part, however, the central contextual point which is addressed by the technological literature is related to the newness of the technologies being used to extend or restructure regimes of surveillance. Thus surveillance is understood to be developing and operating within a context of technological change and advancement. One significant effect of this approach has been a tendency to conceive of surveillance as getting worse over time as technologies develop.

Implicit in this is the notion that surveillance will continue to get worse in the future unless specific action is taken to prevent it from doing so. And, in this case, the kinds of specific actions that are favoured are those that operate at the technological or technical level to disrupt the relationship between surveillance and technology, and, by extension, the relationship between surveillance and power.

Despite some recognition of the context in which surveillance operates, however, Cypherpunks and crypto rebels continue to display a certain naiveté about why surveillance exists, and what benefits and incentives surveillance provides from the point of view of the ones doing the watching. This naiveté is also reflected in the technological literature more broadly. Thus the technological fix which is proposed by these groups and others fails to take into account the divergent interests at stake in any surveillance system.

The sociological literature, by contrast, is very much focused on the interests that operate behind surveillance systems. In particular, that literature has been careful to address the specific social context in which modern surveillance practices have emerged, including its historical emergence as a feature of the modern military, bureaucratic technique, and the organization of the capitalist workplace. Thus the sociological perspective does make significant progress in calling attention to the ways in which the monitoring of employee e-mail produces and reproduces hierarchies within the workplace. Furthermore, it provides at least the beginnings of a framework for thinking critically about the ways in which these localized instances of discipline fit into larger disciplinary patterns. The sociological approach, then, highlights the social *context* of surveillance, as well as its social *effects*. Thus the kinds of solutions that would be suggested by a sociological analysis of the surveillance of employee e-mail would not necessarily address the practice of employee e-mail monitoring itself, but rather the underlying social issues that are reflected and amplified by that practice. These might include the distribution and functioning of power along the lines of class, race, or gender, and the role of social institutions, such as workplaces, in maintaining social order through generalized patterns of discipline.

While an appreciation of the historical and social context of surveillance is clearly apparent throughout much of the sociological literature on surveillance, there

is still a tendency among some analysts to see technology as *the* decisive factor in some sense or another. Thus, for example, both Lyon and Marx argue that there is a new surveillance based largely on what they see as the distinctive characteristics of the new technologies that are being developed and used in surveillance contexts. This claim signals an important tension in the sociological literature around the analysis of the nature and causes of the surveillance problem.

While analysts seem unable to be clear about the relative weight that should be afforded to technological factors as opposed to other social and historical factors in the development of surveillance societies, the sociological literature is quite clear on the point that subjects are controlled and acted upon -- in other words, disciplined -- under broad conditions of surveillance. In such a context, individual action against or resistance to surveillance is essentially futile, since individual action can never seriously threaten the large, organized interests behind surveillance. Furthermore, where the analysis of surveillance has followed along Foucauldian lines, it is not clear where the impulse for resistance would come from, since the disciplinary capacity of surveillance is virtually total.[1] The difficulty of locating a basis for resistance finds expression in the general lack of practical strategies for resistance in the sociological literature on surveillance.[2] Thus we do not find in that literature any kind of practical framework though which to respond to the problem of employee e-mail surveillance. Instead, we find frameworks within which to question how order is produced within the workplace via e-mail surveillance and, more specifically, in which direction power flows in such contexts. But even this analysis is limited, because it deals only with macro issues, and not with the micro issues of how power *actually* function to shape behaviour or to manipulate subjectivities.

The legal, technological, and sociological approaches to theorizing surveillance are clearly valuable analytical tools. They provide important insights into a number of issues which are raised by the practice of employee e-mail monitoring. These issues include the relationship between the right of privacy and the various rights of employers with respect to the monitoring of labour processes

---

[1] Foucault himself was very critical of the totalizing impulse in theoretical work. Nevertheless, it is not clear to me that his own work did not succumb to this impulse in some ways.

[2] It is also reflected, I would argue, in Lyon's rather bizarre and not particularly convincing claim that St. Augustine's other city provides a good basis for resisting (and/or justifying) surveillance. See pp. 212-213.

and labourers, the technological design of e-mail systems and the interests which are served by that design, and the relationship between the specific practice of employee e-mail monitoring and larger patterns of discipline in the workplace and elsewhere. These are clearly significant issues, well worthy of careful consideration and analysis.

The kinds of analysis made possible by these literatures is, however, significantly limited by the fact that there has been virtually no dialogue between them. This has had important implications in terms of how far these analyses have been able to go in assessing the nature and extent of the surveillance problem, and in determining practical, effective strategies of resistance against surveillance. In effect, none of the literatures on surveillance has been able to incorporate the insights of the other literatures. Thus, for example, the legalistic discourse has not incorporated or addressed any of the important contextual work that has been done by the sociologists. By the same token, the sociological literature has not engaged with the kinds of practical legislative or technological solutions proposed by the legalistic and technological literatures. The net effect of this has been that each line of inquiry has developed more or less in a vacuum, and has not been enriched or challenged by interactions with other, differently-oriented kinds of analyses. To the extent that contemporary literatures on surveillance can be said to be stagnating,[3] they will continue to do so for as long as they develop in isolation from one another. Thus, I would argue, it is imperative that some kind of dialogue emerge *between* the literatures on surveillance.

Even the opening up of a dialogue between the literatures on surveillance, however, would not be sufficient to extend the analysis of surveillance to include *all* the salient issues. There are clearly certain issues that are not addressed, and certain patterns that are not accounted for, by the legal, technological, and sociological literatures. Thus, for example, while those literatures do provide some insight into the generalized disciplinary effects of surveillance, they do not address the ontological questions that arise from the interplay of surveillance and subjectivity, even though it seems obvious that surveillance is carried out, and has disciplinary

[3] My use of the word "stagnating" in this context is intended to refer to the fact that each of the surveillance literatures has developed along particular lines of inquiry, more or less without challenge. The term is not meant to imply any judgment on the content of those analyses.

effects, on *subjects*. These questions might include, for instance, the *particular* effects of surveillance upon the subject, the process by which discipline comes to be enacted at the level of subjectivity, and the relationship between discipline and the constitution of subjects. While some of the sociological work has addressed the role of surveillance in producing social order, this work is far from complete, and leaves several important themes, including subjectivity, more or less untouched.

Although the current literatures on surveillance do not, as yet, provide adequate tools with which to address the theme of subjectivity, this theme has figured prominently in other literatures. For my purposes here, the approaches taken by Erving Goffman and those theorists broadly grouped together under the rubric of "post-structuralism" are of particular interest.[4] Goffman, perhaps more than the post-structuralists, has had some influence among certain surveillance theorists[5], though none seem to have applied his model of social interaction to the analysis of the effects of surveillance upon the subject in any sustained kind of way.

Goffman's work is based on the premise that "when an individual appears before others, he [sic] knowingly and unwittingly projects a definition of the situation, of which a conception of himself is an important part."[6] This leads Goffman to

---

[4] The term "post-structuralist" is a highly contested one. As a label, it, like "postmodern," seems to be most often imposed (critically) from the outside upon writings that may or may not be related, and are often incompatible with one another. Judith Butler notes that Jean-François Lyotard champions the term "postmodern," but that "he cannot be made into the example of what all the rest of the purported postmodernists are doing. Lyotard's work is, for instance, seriously at odds with that of Derrida, who does not affirm the notion of "the postmodern," and with others for whom Lyotard is made to stand." [Judith Butler, *Contingent Foundations*, Feminists Theorize the Political. Judith Butler and Joan Scott, eds. (New York and London: Routledge, 1992) pp. 5.]

Following Butler, I use the term post-structuralist to refer to that work which makes the point that "power pervades the very conceptual apparatus that seeks to negotiate its terms, including the subject position of the critic; and further, that this implication of the terms of criticism in the field of power is *not* the advent of a nihilistic relativism incapable of furnishing norms, but, rather, the very precondition of a politically engaged critique...[T]he point is not to do away with foundations, or even to champion a position that goes under the name of antifoundationalism. Both of those positions belong together as different versions of foundationalism and the skeptical problematic it engenders. Rather, the task is to interrogate what the theoretical move that establishes foundations *authorizes*, and what precisely it excludes or forecloses." [Butler, op. cit., pp. 6-7.]

[5] Gary Marx studied under Goffman, and Charles Raab refers to him in his own work on surveillance.

[6] Erving Goffman, The Presentation of Self in Everyday Life. (New York: Doubleday, 1959) pp. 242. I am indebted to Charles Raab for introducing me to Goffman's work and for suggesting its utility for surveillance theory.

suggest that social life can be understood from the perspective of theatrical performance. His Presentation of Self in Everyday Life, then, is a study of "the way in which the individual in ordinary work situations presents himself and his activity to others, the ways in which he guides and controls the impression they form of him, and the kinds of things he may and may not do while sustaining his performance before them." [7] Reading the presentation of self in such contexts as a kind of performance, Goffman is able to derive "dramaturgical principles" of social interaction. These principles provide a framework through which to deliberate on the behavioral modifications that occur when people are aware of being watched, or of the possibility of being watched.[8]

In Goffman's analysis, social interaction is not only as a kind of dramatic performance, but also an *information game* -- "a potentially infinite cycle of concealment, discovery, false revelation, and rediscovery."[9] This game involves "the reciprocal influence of individuals upon one another's actions when in one another's immediate physical presence."[10] Such influence is exerted by way of performances which encompass "all the activity of a given participant on a given occasion which serves to influence in any way any of the other participants" including, where applicable, the audience. [11]

Although Goffman's own study is limited to the management of impressions in *face-to-face social interactions*, his work clearly has significant applications in the study of how people respond to the awareness of real or potential audiences in the context of surveillance and of electronic communications. In particular, some of Goffman's insights into impression management can be fruitfully incorporated into an understanding of how the presence, or possible presence, of an audience impacts the behaviour of the performer who is, in this case, the subject under surveillance. And if we take seriously Goffman's claims about the nature of social interaction, and in particular about its performative nature, then we must, at very least, inquire after

---

[7] Goffman, pp. xi.
[8] On the theme of whether we have, or should have, a right to present ourselves in any way we wish, see the classic article by Richard Posner, "The Right to Privacy," *Georgia Law Review*. 12: 393-422, 1978.
[9] Goffman, pp. 8.
[10] Ibid., pp. 15.
[11] Ibid.

whether the presence or presumed presence of an audience, either in the workplace or in other contexts, has an effect on the subject.

In order to get at what the effects of workplace surveillance on the subject are, or might be, it is useful to consider in more detail Goffman's notion of performance and its relationship to the concepts of identity and subjectivity. This relationship has as its starting point a particular understanding of the performative self, which is apparent in Goffman's elaboration on the theme of masks as metaphors. He suggests that:

> It is probably not mere historical accident that the word person, in its first meaning, is a mask. It is rather a recognition of the fact that everyone is always and everywhere, more or less consciously, playing a role... It is in these roles that we know each other; it is in these roles that we know ourselves.[12]

Goffman goes on to argue that the mask we wear represents "the conception we have formed of ourselves -- the role that we are striving to live up to -- this mask is our truer self, the self we would like to be."[13] But people generally have more than one role to perform, and consequently wear more than one mask. Thus, in the context of the workplace, as in other contexts, the performance we put on may not necessarily represent the conception we have formed of ourselves in its entirety, but rather adherence to socially dictated scripts about what kinds of performances are accepted or expected within particular contexts. This leads Goffman to suggest that "a status, a position, a social place is not a material thing, to be possessed and then displayed; it is a pattern of appropriate conduct, coherent, embellished, and well articulated. Performed with ease or clumsiness, awareness or not, guile or good faith, it is none the less something that must be enacted and portrayed, something that must be realized."[14]

Patterns of appropriate conduct which confer status or mark a place, then, are achieved by the continuous performance of particular roles. Goffman draws

---

[12] Robert Ezra Park, Race and Culture. (Glencoe, Ill.: The Free Press, 1950) pp. 249, as quoted in Goffman, pp. 19.

[13] Goffman, pp. 19. Although Goffman refers to a mask in the singular, there is nothing in his work which suggests that the conception we form of ourselves, and which is expressed through role-playing, must necessarily be singular or static. There is some controversy over what kind of theory of the subject underlies Goffman's analysis. See discussion below.

[14] Goffman, pp. 75.

upon a passage from Sartre's Being and Nothingness to illustrate this point. Having described in extensive detail the movements of a waiter in a café, Sartre writes that:

> All his behaviour seems to us a game. He applies himself to chaining his movements as if they were mechanisms, the one regulating the other; his gestures and even his voice seem to be mechanisms; he gives himself the quickness and pitiless rapidity of things. He is playing, he is amusing himself. But what is he playing? We need not watch long before we can explain it: he is playing at being a waiter in a cafe. There is nothing there to surprise us. The game is a kind of marking out and investigation. The child plays with his body in order to explore it, to take inventory of it; the waiter in the cafe plays with his condition in order to *realize* it. This obligation is not different from that which is imposed on all tradesmen. Their condition is wholly one of ceremony. The public demands of them that they realize it as a ceremony; there is the dance of the grocer, of the tailor, of the auctioneer, by which they endeavor to persuade their clientele that they are nothing but a grocer, an auctioneer, a tailor. A grocer who dreams is offensive to the buyer, because such a grocer is not wholly a grocer...There are indeed many precautions to imprison a man in what he is, as if we lived in perpetual fear that he might escape from it, that he might break away and suddenly elude his condition.[15]

The waiter's performance must be put on again and again, and it must be a coherent and believable performance. The repetitiveness of the performance is a precondition of the realization of the role. Similarly, argues Goffman, it is only by performing our roles, and wearing our masks, that we become the people that we aspire, or are required, to be.

Goffman's point has significant implications for the study of the effects of surveillance in the workplace. His analysis suggests that we perform in conjunction with other performers, or for the benefit of an audience, but that we do not necessarily perform for ourselves alone. Even if or when we do perform for ourselves, the roles we choose are likely to be different than those we choose to perform in the company of others. What is significant about workplace surveillance, then, and about the monitoring of employee electronic mail in particular, is that it expands the realm of interactivity within the workplace by putting an audience before us even when we are physically alone. The employee who knows her e-mail will be read by someone other than the intended recipient must, in effect, perform herself twice simultaneously-- once for the intended recipient of her message and once for

[15] Sartre, in Goffman, pp. 76.

the employer who monitors her mail. The roles she plays for each of these parties may normally be different ones, but they must be balanced against one another under conditions of workplace monitoring. Goffman's study of the presentation of self in the context of the workplace, then, suggests that there are complex questions to be asked about the subjective effects of employee e-mail monitoring; questions that are quite different from the ones that have preoccupied surveillance theorists to date.

So, for example, Goffman's work would lead us to consider whether the presence, or presumed presence, of an unseen audience has an effect on how employees present or perform themselves. In the context of employee e-mail monitoring, this might involve considering whether people write their messages differently (more guardedly, for example, or more formally), avoid certain topics, or refrain from sending messages to particular people or groups. There is certainly some evidence to suggest that this is indeed the case. In 1991, Brown Group, a footwear company based in St. Louis, developed a very strict policy on the use of the company's computer and e-mail systems. The policy stated that "[a]ll computer programs, hardware, and data are the sole property of Brown Group Inc.; any use of the computer or application for other than company and business purposes is expressly prohibited. Contents of E-mail communications will be monitored by our audit department as deemed necessary."[16] The results of the e-mail auditing were almost immediately apparent: "employees became paranoid and were very careful about any messages they sent. They felt like Big Brother was watching."[17] Goffman's work provides a framework through which to address and theorize that reaction.

A sustained application of Goffman's work to the study of surveillance clearly has the potential to highlight some of the issues which have been clouded over or ignored by the current literature. There are, however, some ambiguities in Goffman's work which may have implications for how it might be effectively applied to the study of surveillance. In particular, Goffman's presentation of the theme of masks and masking points to an underlying ambiguity in his conception of the

[16] Fryer and Furger, op. cit., pp. 170.
[17] Ibid.

subject, and of the nature of the relationship between subjectivity and performance. If, as Goffman contends, we perform the selves we aspire to be, then presumably the self can be said to *precede* the performance because it makes a determination as to which performance it will give. At the same time, however, Goffman argues that our performances are, and must be, continuous, although they not necessarily unchanging. If subjects are constantly performing, then the relationship between subject and performance must necessarily be more complicated than Goffman would have us believe, for it seems that, under such circumstances, the subject cannot be known (even to herself) outside the parameters of performance. The argument that selves are continuously expressed by way of performance, then, raises important questions about the nature of subjects and subjectivity. Throughout his work on the presentation of self, Goffman maintains this ambiguity, seeming to oscillate between viewing the subject as ontologically *prior* to the performance and conceiving of the performance as being *constitutive* of the subject.

While Goffman's work presents the relationship between subjectivity and performance as an ambiguous one, this relationship has been characterized somewhat differently by other theorists. Performance and subjectivity have been central themes in Judith Butler's work on gender as imitation, for example. For Butler, gender is a kind of repetitious performance through which (gendered) subjects are continuously constituted. In her analysis of that performance, Butler suggests that "if the "I" is the effect of a certain repetition, one which produces the semblance of a continuity or a coherence, then there is no "I" that precedes the gender that it is said to perform; the repetition, and the failure to repeat, produce a string of performances that constitute and contest the coherence of that "I.""[18]

While Butler specifically limits her analysis to the question of gender, her work can be applied to other forms of self-presentation. And it has interesting implications for the study of surveillance and subjectivity, since it suggests that one of the things that must be considered is how performances put on for the benefit of those monitoring us might come to constitute us in a variety of subtle yet insidious

[18] Judith Butler, *Imitation and Gender Insubordination* in Inside/Outside. Diana Fuss, ed. (New York: Routledge, 1991.) pp. 18.

ways. Such an analysis would lend greater depth to the claim that power functions through surveillance to discipline subjects.

The concept of the presentation of self, and of performance more generally, clearly provides a useful framework within which to consider questions about the effects of surveillance which are not generally considered within the parameters of the present literature on surveillance. In particular, the notion of self-presentation as performance suggests that one potentially fruitful avenue of inquiry would be to consider whether and how behaviour is changed by the presence, or presumed presence, of an employer's watchful eye. Depending upon how one conceives of the relationship between subjects and performances, such changes in behaviour may be extremely significant. For, if subjects are constituted by their performances, then changes in performance as a result of surveillance signify that power is functioning to constitute subjects differently. An awareness of this functioning would necessarily be reflected in debates about appropriate or adequate protections against surveillance.

While the theme of performance is certainly one way of getting at issues of subjectivity under surveillance, post-structuralists also provide another framework for getting at these issues by way of the theme of communication. This theme, in some ways, builds upon and expands the utility of the concept of performance for an analysis of surveillance, but at the same time is suggestive in its own distinct ways. In particular, it suggests that we might theorize surveillance as a *communicative structure*, and then proceed to interrogate that structure's language and how it enables the functioning of power in particular ways. In this task, Mark Poster's work in The Mode of Information is highly suggestive.

Poster's book is organized around the thesis that history can be periodicized by variations in the structure of symbolic exchange, and that the current (Western) culture gives a "fetishistic" importance to information.[19] He argues that every age "employs forms of symbolic exchange which contain internal and external structures, means and relations of signification. Stages in the mode of information may be tentatively designated as follows: face to face, orally mediated exchange; written

[19] Mark Poster, The Mode of Information. (Cambridge: Polity Press, 1990), pp. 6.

exchanges mediated by print; and electronically mediated exchange."[20] In each stage, the mode of information both articulates and produces a particular kind of subject. "In the first, oral stage, the self is constituted as a position of enunciation through its embeddedness in a totality of face-to-face relations. In the second, print stage the self is constructed as an agent centered in rational/imaginary autonomy. In the third, electronic stage, the self is decentered, dispersed, and multiplied in continuous instability."[21]

This third, electronic stage is of particular interest to me here, both because it captures some of the dynamics of electronic communication in the form of electronic mail, and because my central problem here - the monitoring of employee e-mail - is an instance of electronic communication. Theorized as a form of communication, surveillance is somewhat unique in that information generally flows only in one direction (from the watched to the watcher) and, more significantly, that it is the *receiver* of the information who exerts power in these circumstances. Thus surveillance is different, for example, from propaganda, where information also flows only in one direction, but where power rests with the *producer* and not the *consumer* of information.

On the theme of language, Poster suggests that while it is, to some extent, a tool for intentional action, it "has another, very different capacity: it is a figurative, structuring power that constitutes the subject who speaks as well as the one that is spoken to."[22] Poster further notes that "[e]lectronically mediated communication has compelling effects at this level of language. By distancing the relation of speaking body to listening body, by abstracting from the connection between the reader or writer and the palpable materiality of the printed or handwritten text, electronically mediated communication upsets the relation of the subject to the symbols it remits or receives and reconstitutes this relation in drastically new shapes. For the subject in electronically mediated communication, the object tends to become not the material world as represented in language but the flow of signifiers itself."[23] The shifting relationship between subjects and signifiers as a result of the expansion of

---

[20] Ibid.
[21] Ibid.
[22] Ibid., pp. 14.
[23] Ibid., pp. 14-15.

electronic communications, in e-mail as well as in other forms, has also been noted by other scholars, including William Mitchell on the excellent City of Bits web page. Mitchell notes that, in electronic communications, our disembodied electronic identities are constructed "alias by alias, bit by bit," as a product of all of our various interactions, and of the roles we play or the functions we perform in each of these interactions.[24] Thus our names "float around without precise, unambiguous attachment to unique things, [and] referential complexities abound."[25] In this way, electronic communications throw into question the notion that subjects are centred and stable. The surveillance of these communications in the form of employee e-mail monitoring adds a particular political subtext to the constitution of subjects as such. Clearly, then, the flow of information in the context of employee e-mail surveillance - the language of surveillance, if you will - is highly politicized, and warrants careful consideration.

In Poster's analysis, the emergence of electronic communications contributes to the growing critique of the notion of the subject as stable and centred, suggesting instead that subjects are more accurately conceptualized as fluid, multiple, and discontinuous. This critique must, in my opinion, inform projects to situate surveillance within particular historical or political contexts, for any analysis of the effects of surveillance on the subject must be sensitive to the kind of subject that is at issue, or is thought to be at issue.

It is here, then, that Poster's work has applications in, and implications for, the study of surveillance. His linking of structures of communication with particular characterizations of the subject highlights the fact that communication is a central variable in the constitution of subjects, and in the experience of subjectivity. So if surveillance is a kind of communicative structure in itself, or if it mimics or mirrors certain kinds of communicative structures, then we can reasonably expect it to have effects at the level of subjectivity, and Poster's work provides a vehicle through which to get at what some of these effects might be. Furthermore, Poster makes the point that electronic communications are associated with subjects who are

---

[24] City of Bits WWW Team, City of Bits. Http://www-mitpress.mit.edu/city_of_bits/welcome.html. See section entitled "Corporeal/Incorporeal."
[25] Ibid.

"decentered, dispersed, and multiplied in continuous instability."[26] Electronic communications in themselves, then, have effects upon subjects. The surveillance of these communications might well double their disciplinary or constitutive effect by adding another discursive layer where the functioning of power is reinforced.

If one takes seriously the suggestion that surveillance works to constitute subjects in particular ways, either as particular kinds of subjects, such as workers or consumers, or, more profoundly, as subjects who are multiple, dispersed, and discontinuous, then one must also, I think, consider the hypothesis that what are generally referred to as modern surveillance societies are, in fact, sites of "hypersurveillant control."[27] Here "the prefix "hyper" implies not simply an intensification of surveillance, but the effort to push surveillance technologies to their absolute limit. That limit is an imaginary line beyond which control operates, so to speak, in "advance" of itself and where surveillance -- a technology of exposure and recording -- evolves into a technology of *pre*-exposure and *pre*-recording, a technical operation in which all control functions are reduced to modulations of preset codes."[28] This is precisely the theme of William Bogard's new book, The Simulation of Surveillance. In that work, Bogard's principal concern is with how technologies of simulation function as part of what he refers to as the "imaginary" of surveillant control; the "fantastic dream of seeing everything capable of being seen, recording every fact capable of being recorded, and accomplishing these things, whenever and wherever possible, *prior* to the event itself."[29]

Bogard's characterization of hypersurveillant societies captures something of the layering effect that occurs when electronic communications are subject to surveillance. It is through this layering of the disciplinary effect of surveillance that the imaginary of surveillant control is increasingly realized; the disciplining of subjects through surveillance is not event-based, but rather works continuously to constitute subjects in particular ways. In doing so, it manipulates events long before they ever happen, or are prevented from happening. *This* is the "fantastic dream" of

---

[26] Poster, op. cit., pp. 6.
[27] William Bogard, The simulation of surveillance: Hypercontrol in telematic societies. (Cambridge University Press: Great Britain, 1996), pp. 4.
[28] Ibid.
[29] Ibid., pp. 4-5. Emphasis added.

surveillance; a dream which is being increasingly realized in a variety of contexts.[30] Significantly, it is a dream which has little to do with privacy or technology, and a lot to do with subjectivity. And it is here that the literature on surveillance has failed most markedly; it has been unable to address or confront the fantasy of surveillance because it has been unable to come to terms with the extent to which surveillance has as one of its primary goals the constitutive manipulation of subjects. Broadly speaking, this failure has had two important implications. First, it has meant that, despite extensive debate, the literature on surveillance actually has little to say about whether or not surveillance, as we now experience it, is new. The failure to take subjectivity seriously has meant that the tests of newness are, in real terms, largely irrelevant. This has led to a second important effect: the strategies of resistance which have been developed in response to surveillance have been largely ineffectual, and have certainly not addressed any of the fundamental ontological questions that are raised by a consideration of the constitutive role of surveillance in shaping subjects.

That being said, there are some ostensibly good reasons why this work has *not* been done. Perhaps the most significant of these is that framing surveillance as a problem of subjectivity makes it decidedly more difficult to develop appropriate or adequate strategies of resistance. Framing the problem as one of law, technology, or society, by contrast, allows for the development of legal, technological, or social solutions. And, significantly, each of the literatures on surveillance frames the problem in such a way as to claim a certain privileged understanding of what the problem *really* is and, by extension, what the solution must be. This is particularly apparent among the technologists, for example, whose claim to a better understanding of the admittedly complicated technologies of surveillance is central to their reliance on technology as a form of resistance, and has the effect of marginalizing other views of the surveillance problem.

While privacy, data protection, and encryption technologies may each have their own difficulties, they nevertheless do provide some satisfaction in terms of their concrete, practical appeal. Even if they do not address what I have argued here are

---

[30] Most notably, of course, in the consumer surveillance industry. See Gandy, op. cit., on this point.

the underlying issues, they provide a sense that something is being done and, more significantly, that something *can* be done. In effect, then, much of the literature on surveillance frames the problem in such a way as to make it appear critical and immediate, but nonetheless manageable. Subversion of the constitutive effect of surveillance, however, is a far more ambitious project, and one which is probably less likely to spark public interest or support.

Whatever the appeal of the literature on surveillance may be, failure to consider seriously the theme of subjectivity prevents that literature from every moving beyond "Band-Aid solutions" to the surveillance problem. Even more significantly, the failure to consider, in some detail, questions about the relationship between surveillance and subjectivity seriously hampers our ability to understand what surveillance is and what it does. And it is for this reason that I maintain that an intersection of post-structuralist and surveillance theories would yield powerful insights into surveillance, and in particular into the *effects* of surveillance at the level of subjectivities. Armed with these insights, analysts might begin to make meaningful progress in determining truly effective strategies of resistance against the power that functions through surveillance.

Selected Bibliography

Adorno, Theodor. *The Culture Industry*. New York and London: Routledge, 1992.

Aiello, John R. "Computer-based work monitoring." *Journal of Applied Social Psychology* 23:499-507, April 1 '93.

-- and Carol Svec, "Computer monitoring of work performance." *Journal of Applied Social Psychology* 23:537-48, April 1 '93.

Allen, Anita L. and Erin Mack. "How Privacy Got its Gender," *Northern Illionois University Law Review*. 10: 441-78.

Altman, Irwin. "Privacy: A Conceptual Analysis," *Environment and Behaviour*. Vol. 8 No. 1, March 1976.

Barlow, John Perry "Jackboots on the Infobahn," *Wired*. April 1994: 40-8.

Baudrillard, Jean. *The Ecstacy of Communication*. New York: Semiotext(e), 1987.

-- *For a Critique of the Political Economy of the Sign*. St. Louis: Telos Press, 1981.

Bauman, Zygmunt. *Freedom*. Minneapolis: University of Minnesota Press, 1988.

-- *Intimations of Postmodernity*. New York and London: Routledge, 1992.

Bell, Daniel. *The Coming of Post-Industrial Society*. New York: Basic Books, 1973.

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

Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca and London: Cornell University Press, 1992.

-- "Computers, Personal Data and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990's," *Science, Technology and Human Values*. 16: 51-69.

-- *The Political Economy of Privacy: A Review of the Literature*. Hackensack: Center for Social and Legal Research, 1995.

Bernstein, Richard J. *The New Constellation: The Ethical-Political Horizons of Modernity/Postmodernity*. Cambridge, UK: Polity Press, 1991.

Bjerklie, David. "E-Mail: The Boss is Watching." *Technology Review*. April 1993, Volume 96, Issue 3.

Bleecker, Samuel. "The Virtual Organization." *The Futurist* 28:9-12+, Mar/Apr '94.

Burnham, David. *The Rise of the Computer State*. New York: Random House, 1980.

Butler, Judith and Scott, Joan (Eds.). *Feminists Theorize the Political.* New York and London: Routledge, 1992.

Campell, Duncan and Connor, Steve. *On the Record: Surveillance, Computers and Privacy.* London: Michael Joseph, 1986.

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

Chaum, David. "Achieving Electronic Privacy," *Scientific American.* August 1992: 96-101.

Clarke, Roger A. "Information Technology and Dataveillance," *Communications of the ACM* 31: 498-512.

Dandeker, Christopher. *Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day.* New York: St. Martin's Press, 1990.

Davies, Simon. *Big Brother: Britain's Web of Surveillance and the New Technological Order.* London: Pan Books, 1996.

Decker, K.H. *Employee Privacy Law And Practice.* New York: John Wiley, 1987.

Detienne, Kristen Bell. "Big Brother or Friendly Coach?" *The Futurist* 27:33-7 September/October 1993.

Ellul, Jacques. *The Technological Society.* New York: Vintage Books, 1964.

Flaherty, David H. "Workplace Surveillance: The Emerging Reality." In William Kaplan, Jeffery Sack, Morley Gunderson (eds.) *Labour Arbitration Yearbook 1992.* Toronto: Butterworths - Lancaster House, 1992.

-- *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill, N.C.: University of North Carolina Press, 1989.

Fenner, Deborah B., F. Javier Lerch and Carol T. Kulik. "The Impact of Computerized Perfomance Monitoring..." *Journal of Applied Social Psychology* 23:573-601, Apr 1 '93.

Forester, Tom (ed.). *The Information Technology Revolution.* Oxford: Basil Blackwell, 1985.

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

Franklin, Ursula. *The Real World of Technology.* Ontario: Anansi Press, 1992.

Frey, Bruno. "Does Monitoring Increase Work Effort?" *Economic Inquiry* 31:663-70, Oct '93.

-- "Shirking or Work Morale? The Impact of Regulating." *European Economic Review* 37:1523-32, Dec '93.

Gandy, Oscar. *The Panoptic Sort.* Boulder: Westview Press, 1992.

Gannon Shoop, Julie. "Electronic Monitoring: Is Big Brother at the Office?" *Trial* 28:13-15, Jan '92.

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

Gilfoyle, Timothy. "The Moral Origins of Political Surveillance: The Preventive Society in New York City." *American Quarterly* 38:637-651, Fall 1986.

Giddens, Anthony. *Social Theory and Modern Sociology.* Cambridge: Polity Press, 1987.

-- *The Consequences of Modernity.* Cambridge, UK: Polity Press, 1990.

-- *The Nation State and Violence.* Cambridge, UK: Polity Press, 1985.

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

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

Griffith, Terri L. "Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring." *Journal of Applied Social Psychology* 23:549-72, April 1 '93.

Hammonds, Keith et al. "E-mail: Beware of Big Brother." *Business Week.* 3/4/96, Issue 3465.

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

-- *The Equifax Canada Report on Consumers and Privacy in the Information Age.* Quebec: Equifax Canada Inc., 1992.

Herring, Susan. *Gender Differences in Computer-Mediated Communication: Bringing Familiar Baggage to the New Frontier.* Electronic document, available at gopher://gopher.cpsr.org:70/ /00/cpsr/gender/herring.txt.

-- "Gender Differences in Computer-Mediated Communication and also Politeness in Computer Culture: Why women thank and men flame," *Communicating Across Cultures: Proceedings of the Third Berkeley Women and Language Conference.* Bucholtz and Sutton, eds. Berkeley Women and Language Group.

Hoffman, Lance, ed. *Building in Big Brother: The Cryptographic Policy Debate.* New York: Springer-Verlag, 1995.

Hughes, Eric. *A Cypherpunk's Manifesto.* Electronic document, available at http://weber.u.washington.edu/~phantom/cpunk/cpunk.manifesto.

Information and Privacy Commissioner/Ontario. *Workplace Privacy: The Need for a Safety-Net.* November 1993.

-- *Workplace Privacy: A Consultation Paper.* June 1992.

-- *Privacy Protection Principles for Electronic Mail Systems*, February 1994.

Ippel, Pieter, de Heij, Gaus and Crouwers, Bart (Eds.). *Privacy Disputed.* The Hague: Registratiekamer, 1995.

Jankanish, Michele. "Monitoring and surveillance in the workplace: Privacy issues in an international perspective" *Conditions of Work Digest.* Volume 12, Number 1, 1993

Jenkins, Jolyon. "Eye Can See You." *New Statesman and Society* 5:14-15, Feb 21 '92.

Kantrowitz, Barbara and McKay, Betsy. "Who Holds the Key to the E-mailbox?" *Newsweek.* 12/20/93, Volume 122, Issue 25.

Laudon, Kenneth C. *Dossier Society.* New York: Columbia University Press, 1986.

Lee, Laurie Thomas. "Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop," *The John Marshall Law Review.* Volume 28:137.

Levy, Stephen. "The Encryption Wars: Is Privacy Good or Bad?" *Newsweek*, April 24, 1995.

-- "Crypto Rebels," *Wired.* Electronic document available at http://www.eff.org/pub/Privacy/crypto_rebels.article. Also appeared in printed form in Wired magazine, issue 1.2.

Linklider, J.C.R. et al, "The Computer as a Communication Device," *International Science and Technology.* April 1968

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

-- "An Electronic Panopticon?" *The Sociological Review* 41:653-78, Nov '93.

-- "Bentham's Panopticon: From Moral Architecture to Electronic Surveillance," *Queen's Quarterly* 98/3 (Fall 1991), pp. 600.

Marx, Gary. *Undercover: Police Surveillance in America.* Berkeley: University of California Press, 1988.

-- "The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures", in James F. Short, Jr. (Ed.). *The Social Fabric: Dimensions and Issues.* Beverly Hills: Sage Publications, 1986.

-- "I'll Be Watching You: Reflections on the New Surveillance" in *Dissent 22.*

Marx, Karl and Engels, Friedrich. "Manifesto of the Communist Party" in Robert C. Tucker, ed. *The Marx-Engels Reader: Second Edition*. New York and London: W.W. Norton and Company, 1978.

May, Timothy. *The Crypto Anarchist Manifesto*. Electronic document, available at http://weber.u.washington.edu/~phantom/cpunk/crypto.anarch.manifesto.

Meeks, Brock N. "The End of Privacy." Early release electronic document, available through *Wired Online/Hotwired*, http://www.hotwired.com/frontdoor. Final draft appeared in printed form in *Wired* magazine, issue 2.04, April 1994.

Miller, Arther R. *The Assault on Privacy*. Ann Arbor: University of Michigan Press, 1971.

Nebeker, Delbort and Charles Tatum. "The Effects of Computer Monitoring" *Journal of Applied Social Psychology* 23:508-36 April 1 '93.

Niebel, Benjamin W. *Motion and Time Study* (Eighth Edition). Illinois: Irwin Publishing, 1988.

Organization for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*. Paris: OECD, 1981.

Ottensmeyer, Edward J. and Mark A. Heroux. "Ethics, Public Policy, and Managing Advanced Technologies." *Journal of Business Ethics* 10: 519-26, Jul '91.

Pacey, Arnold. *The Culture of Technology*. Oxford: Blackwell, 1983.

Paden, Roger. "Surveillance and Torture: Foucault and Orwell on the Methods of Discipline." *Social Theory and Practice* 10:261-271, Fall, 1984.

Piller, Charles. "Bosses with X-Ray Eyes," *Macworld*, July 1993.

Posner, Richard A. "The Right to Privacy," *Georgia Law Review*. 12: 393-422, 1978.

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

Privacy Committee of New South Wales. *Invisible Eyes: Report on Video Surveillance in the Workplace*. Sydney: Privacy Committee of New South Wales, 1995.

Privacy Protection Study Commission. *Personal privacy in an information society: The report of the Privacy Protection Study Commission*. Washington: Government Printing Office, 1977.

Rothfeder, Jeff. *Privacy for Sale*. New York: Simon and Shuster, 1992.

Rule, James B., et al. "Documentary Identification and Mass Surveillance in the United States", *Social Problems* 31: December 1983.

-- "High-Tech Workplace Surveillance: What's Really New?" in David Lyon and Elia Zureik, (Eds.) *Computers, Surveillance and Privacy*. Minneapolis and London: University of Minnesota Press, 1996.

-- et al. *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. New York: Elsevier, 1980.

Shaw, Erin et al. *The Privacy Handbook: A Practical Guide to your Privacy Rights in British Columbia and How to Protect Them*. Vancouver: B.C. Civil Liberties Association and B.C. Freedom of Information and Privacy Association, 1994.

Simitis, Spiros. "Developments in the Protection of Workers' Personal Data" in *Conditions of Work Digest: Workers' Privacy, Part 1*. Geneva: International Labour Office, 1991.

Tapscott, Don. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. New York: McGraw Hill, 1996

-- *Paradigm Shift: The New Promise of Information Technology*. New York: McGraw Hill, 1992.

Turkle, Sherry. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schuster, 1995.

U.S Congress, Office of Technology Assesment. *Information Security and Privacy in Network Environmnets*. OTA-TCT-606. Washington DC: U.S. Government Printing Office, 1994.

-- *The Electronic Supervisor: New technology, new tensions*. OTA-CIT-333. Washington, D.C.: U.S. Government Printing Office, 1987.

Wajcman, Judy. *Feminism Confronts Technology*. Pennsylvania: The Pennsylvania State University Press, 1991.

Warren, Samuel and Brandeis, Louis. "The Right to Privacy," *Harvard Law Reveiw* 4 1890.

Weber, Max. "The Meaning of Discipline and Bureaucracy," *From Max Weber: Essays in Sociology*. H.H. Gerth and C. Wright Mills, (Eds.). New York: Oxford University Press, 1958.

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

Will, Ian. *The Big Brother Society*. London: Harrap, 1983.

John Whalen, "You're Not Paranoid: They Really Are Watching You," *Wired*. March 1995.

White, Victoria A. "Ethical Implications of Privacy in Electronic Mail," *Proceedings of Technical Conference on Telecommunications R&D in Massachusetts*, University of Massachusetts Lowell, October 25, 1994.

Wiegner, Kathleen. "The Trouble with E-mail," *Working Woman*. April 1992.

Winner, Langdon. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, Massachusets: The MIT Press, 1978.

-- "Who will we be in cyberspace?" *The Network Observer*. Volume 2, Number 9, September 1995.

-- *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press, 1986.

VITA

Surname: Kahale **Given Names**: Sandra Diane

Place of Birth: Montreal, Quebec, Canada

Educational Institutions Attended:

University of Victoria	1993 to 1996
University of Western Ontario	1989 to 1993

Degrees Awarded:

B.A. (Honours)	University of Western Ontario	1993

PARTIAL COPYRIGHT RELEASE

I hereby grant the right to lend my thesis to users of the University of Victoria Library, and to make single copies only for such users or in response to a request from the Library of any other university, or similar institution, on its behalf or for one of its users. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by me or a member of the University designated by me. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Title of Thesis:

(Be)Labouring the Subject: Employee E-Mail Surveillance and the Limits of Surveillance Theory

Author [redacted]

Sandra Diane Kahale
September 15, 1996