INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI®

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

Electronic Surveillance and the Prospects for Privacy in Canada's Private Sector by the Year 2000

by
Miyo Yamashita

Graduate Program in Communications
McGill University, Montreal

A thesis
submitted to the Faculty of Graduate Studies and Research
in partial fulfilment of the requirements for the degree
of Doctor of Arts in Philosophy

March, 1998

Abstract

This dissertation is concerned with surveillance, which refers to the monitoring and supervision of populations for specific purposes. Of special interest are the ways in which new technologies are augmenting the power of surveillance in the late twentieth century, and therefore influencing the privacy debate. Three things are noted about this. First, large-scale surveillance by bureaucratic organizations is a product of modernity, not of new technologies. This is evident from Part I of the dissertation, which argues that increased surveillance capacity comes as a result of specific economic and political circumstances that favour the use of technological systems of particular kinds, which invariably feature enhanced capacities. Second, surveillance has two faces; advantages appear alongside serious disadvantages. This is also evident in Part I of the dissertation which suggests that much surveillance theory is dystopian and therefore, an incomplete paradigm. Finally, new technologies facilitate some major magnification of surveillance power; some even argue that they change its character qualitatively. As such, privacy features prominently alongside discussions of electronic surveillance. This is evident in the final two parts of the dissertation which evaluate privacy as a strategy for limiting electronic surveillance. In this regard, Part II examines *technical* challenges to electronic surveillance, expressed through privacy law in particular, and Part III analyses *mobilization* challenges, which have to do with the role played by social movements in attempting to bring about broader-based change than mere legislation. Throughout the dissertation, the argument is made that surveillance has become a central feature of contemporary advanced societies and as such, it should be a major concern of both social analysis *and* political action. This is why the dissertation is divided into distinct, but overlapping, parts, with the first part focusing on social and critical theory, and the second and third parts focusing on the public policy arena. By organizing the dissertation in this manner, it is demonstrated that the issues raised by surveillance must no longer be treated in a marginal, piecemeal fashion; no longer, that is, if we wish to avoid a dystopian future. The analysis offered in this dissertation will make a notable contribution to avoiding that future by defining the social and historical meanings of electronic surveillance so that, in dialogue with it, more room will be made for just, fair, and responsible political practice.

Résumé

La thèse porte sur la surveillance, c'est-à-dire le contrôle et la supervision des populations à des fins spécifiques. Une importance particulière est accordée à la façon dont les nouvelles technologies accroissent les possibilités de surveillance à la fin du 20e siècle, influençant de ce fait le débat sur la protection de la vie privée. Trois éléments fondent notre réflexion. Premièrement, la surveillance à grande échelle par les organisations bureaucratiques apparaît avec la modernité, donc bien avant l'émergence des nouvelles technologies. Cet aspect est plus particulièrement abordé dans la première partie, qui pose l'hypothèse selon laquelle l'augmentation des capacités de surveillance résulte d'une conjoncture économique et politique favorisant le recours à des systèmes technologiques particuliers dont les performances sont forcément accrues. Deuxièmement, les effets de la surveillance sont doubles; les avantages qu'elle procure sont indissociables des sérieux inconvénients qu'elle comporte. Dans la première partie de la thèse, nous faisons également la démonstration qu'une part significative des théories de la surveillance s'avère dystopique, et qu'en conséquence, elle est un paradigme incomplet. Finalement, les nouvelles technologies favorisent une glorification du pouvoir de surveillance. Certains affirment même qu'elles en modifient qualitativement le caractère. La question de la protection de la vie privée est ainsi au coeur des débats à propos de la surveillance électronique. Les deux dernières parties de la thèse abordent ainsi la question de la protection de la vie privée comme stratégie pour limiter la surveillance électronique. Dans cette perspective, la deuxième partie de la thèse examine le défi technologique de la surveillance électronique, par l'étude des mesures légales mises en place pour protéger la vie privée. La troisième partie analyse le défi de la mobilisation, en examinant le rôle que pourraient jouer les mouvements sociaux pour apporter des améliorations plus globales, allant au-delà du seul plan législatif. L'ensemble de la thèse démontre que la surveillance est devenue un élément central des sociétés contemporaines développées, et que conséquemment, elle devrait être appréhendée à la fois comme un objet d'analyse sociale et d'action politique. Ces deux perspectives sont à l'origine du plan de la thèse, qui se déploie en deux chapitres distincts mais dont les contenus se superposent partiellement. La première partie est centrée sur les théories sociales et critiques, alors que la deuxième et la troisième partie s'attardent plutôt à l'examen des mesures publiques. En structurant le propos de la sorte, nous démontrons que pour minimiser les conséquences sur l'avenir des citoyens, les enjeux de la surveillance doivent être envisagés non plus de façon marginale et isolée. Nous croyons que l'analyse proposée ici contribuera à désamorcer les conséquences néfastes de la surveillance en définissant plus adéquatement les implications socio-historiques du phénomène. En étudiant le phénomène dans ses interrelations, la surveillance électronique pourra être envisagée dans sa globalité et résulter en des pratiques plus justes et plus responsables.

Acknowledgements

In acknowledging the help I received in writing this dissertation, I must begin with my supervisor, Dr. Gertrude Robinson. She not only read and expertly critiqued every chapter, but discussed with me the major ideas, intellectual and political. I am indebted to her for her support, guidance, and trust throughout the entire process, and for her caring, professional manner which I hope to emulate in my own career as a scholar.

A number of other people have also been extremely helpful in writing this dissertation and they deserve sincere thanks. At McGill, where the research and writing for the dissertation took place, strong encouragement came from Dr. Charles Levin and Dr. Will Straw, as well as from Dr. Berkeley Kaite who has involved me in numerous engaging conversations on feminism, film studies, and masculinity since I first entered the Graduate Program in Communications as a Master's student in 1991. In addition, I would like to thank Marie-Anne Poussart for translating the abstract, and Lise Ouimet and Pierre Gaudrault for helping me to navigate the numerous bureaucratic trails one must follow in the course of a graduate student's career. They have assisted in this navigation with consistent patience, humour, and optimism. Fellow graduate students at McGill must also be saluted for their care and enthusiasm, in particular, Rebecca Sullivan and Bart Beaty.

Financially, I have been supported by a doctoral fellowship from the Social Sciences and Humanities Research Council of Canada. My greatest debt, however, is emotional. I am deeply grateful for the love enjoyed with my friends and family - Amalia, Caryn, Kathy, Heather, Howard, Joel, Joanne, Judy, Vicki, my parents, brother, and grandmothers. The time spent with these people eating our favourite Japanese dishes, reading books and magazines, watching movies, and laughing and crying together, is as much my life as the dissertation in your hands. I would also like to thank Joe for his loving support, which has forever changed the way I see the world. Finally, I want to thank Ian, who, in the short time I have known him has already redefined some of the most important and beautiful words in the English language - joy, hope, serenity, and love.

Table of Contents

Chapter One: Introduction and Literature Review

Focus

Great excitement was generated during the 1970s and early 1980s about the arrival of new social conditions. Computer and communications technologies had made possible the "Information Society". All manner of benefits awaited us; new prosperity, new democratic and educational opportunities, a "global village" thanks to new telecommunications, and a realignment of workplaces and class relations. There is no denying that advantages do accrue from such technological development, but a little historical reflection and critical imagination makes warning bells ring.

A number of writers - including David Lyon (1988), Heather Menzies (1996), and Frank Webster (1993) - took it upon themselves to assess just what was going on in the so-called information revolution. Most of them argued that each situation should be analysed in its own right, that new technologies may well be implicated in some radical social changes that we do not yet understand fully, but that utopian dreams of wholesale societal megashifts were at best misleading hyperbole and at worst dangerous delusions.

Since then, the debates surrounding new technologies have tended to become much more sober, it not sombre. The failure of computer-based service economies to lift the world out of recession, the advent of electronic war, and the dismayed realization that computers have a huge capacity to track the tiny details of our personal lives, have all helped foster more forbidding social forecasts. Even fearing the spectre of "Big Brother" scarcely seems to do justice to the new mood. The term "surveillance society" was first coined in 1985 by James Rule; the warning note is growing in volume.

Of all the questions raised by new technologies, the one that strikes me as being most socially pervasive is the garnering of personal information to be stored, matched, retrieved, processed, marketed, and circulated using powerful computer databases. The result of my investigation is this dissertation, in which I examine the major dimensions of what we now speak of as "surveillance". Whereas once this had a fairly narrow meaning, to do with policing or espionage, surveillance is used here as a shorthand term to cover the many, and expanding, range of contexts within which personal data is collected by employment, commercial, and administrative agencies, as well as in policing and security.

Throughout the dissertation, I argue that surveillance has become a central feature of contemporary advanced societies and as such, it should be the focus of both social analysis *and* political action. To this end, the dissertation is divided into three parts, each of which has two chapters. Part I traces the history of surveillance from the modern era and outlines the major theories of surveillance that contribute to our present day understanding of the relationship between technology, privacy, and public policy. Part II describes the background conditions and proximate events that have made the announcement of Canadian privacy legislation for the private sector possible. In May 1996, the Minister of Industry, John Manley, announced a number of government decisions about the future character of the "information highway". Buried within these decisions was the conclusion that "the right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens" (Industry Canada, 1996: 25). Hence:

> As a means of encouraging business and consumer confidence in the Information Highway, the Ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

At the present time, nobody knows the depth of the federal government's commitment to this issue. Moreover, there has been little detailed policy analysis of what a "legislative framework" might look like and very little public debate (Bennett, 1996). Nevertheless, the announcement does constitute a significant triumph for the small "advocacy coalition" (Sabatier, 1988) of privacy and data protection commissioners, academics, public interest groups, and individual bureaucrats that have been arguing for a more effective and consistent set of "rules of the road" (Bennett, 1996) for the treatment of personal data in Canada.

Finally, Part III examines challenges to surveillance in the late twentieth century in the form of "awareness movements". It highlights the ways in which so-called submerged networks become temporarily visible and mobilize around a key issue, thereby indicating that countervailing forces against surveillance do exist, though not necessarily in the form of conventional pressure groups, lobby groups or political parties. In this respect, resistance to contemporary surveillance is different - and less effective - than resistance to other social problems. For this reason, Part III also examines a "successful" public awareness movement in another field: breast cancer. It is hoped that from such an analysis privacy advocates and scholars may be able to do some "lesson-drawing" (Bennett, 1990) for their own pursuits in raising public consciousness about surveillance.

Two questions are at the forefront of the dissertation. First, why is privacy legislation for the private sector in Canada "an idea whose time has come?"[1] And second, how can public awareness about surveillance be increased? These questions are of the utmost importance because, as I noted earlier, ordinary people now find themselves, to an unprecedented extent, "under surveillance" in the routines of everyday life. Surveillance, as described here, concerns the typical, mundane, 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 a book from the library, or crossing a border on trips abroad. In each case mentioned, computers record our transactions, check against other known details, ensure that we and not others are billed or paid, store bits of our biographies, or access our financial, legal, or national standing. Thus, computers and their associated communications systems now mediate a host of "ordinary" relationships; as such, to participate in modern society is to be under electronic surveillance.

Part I: Situating and Understanding Surveillance

Surveillance did not develop overnight. Part I argues that ever since modern governments started to register births, marriages, and deaths, and ever since modern businesses began to monitor work and keep accurate records of employees' pay and

---

[1] Speech by Tom Wright, former Information and Privacy Commissioner of Ontario, to the *Information Issues and Access in Transition: Access and Privacy '97 Conference*, Ottawa, Ontario, January 28, 1997. Mr. Wright suggested that legislation for the private sector in Canada is "an idea whose time has come".

progress, surveillance has been expanding. In addition, the electronic component of surveillance is, in one limited sense, nothing new. Wiretapping and other forms of message interception have been the common currency of espionage and intelligence services for many decades. However, in the late twentieth century, electronic technologies have been widely introduced in order to augment and sustain surveillance activities on an even broader basis than that known in the era of typed documents, printed regulations, and index cards. There are suspicions that such surveillance portends a "new" situation.

However, such suspicions cannot be confirmed or denied without reference to the long-term historical context. Part I outlines this context by suggesting that surveillance as we know it today - that is, as an institutionally central and pervasive feature of social life - did not emerge until modern times. While its primitive forms may be seen, for instance, in the eleventh century with the Domesday Book, its expansion from the nineteenth century was dramatic. Systematic surveillance, on a broad scale as understood here, came with the growth of military organization, industrial towns and cities, government administration, and the capitalist business enterprise within European nation-states. It was, and is, a means of power; but not merely in the sense that surveillance enhances the position of those "in power."

Paradoxically, as seen in Part I, surveillance expanded with democracy. Indeed it is associated with the post-Enlightenment "demand for equality" (Dandeker, 1990), and with populations previously denied access to full political involvement. In this respect, surveillance may be viewed as the other side of the coin of democracy. As citizens demanded equal rights and participation in the modern nation-state, they were subject to

identification, registration, and documentation in proliferating dossiers. In this vein, Alexis de Tocqueville astutely observes that modern mass democracies depend upon an expanded range of bureaucratic administrative tasks. Ironically, suggests de Tocqueville, democracy produces privatized citizens whose paramount concern is personal welfare. This renders such individuals particularly vulnerable to the crushing strength of central state institutions (1968). As surveillance develops, so individual anxiety about "privacy" emerges, stimulated by what are felt as the encroachments of government administration.

Historically, then, the development of surveillance is complex. This may explain the relative lack of countervailing organizations committed to investigating, and if necessary resisting, its spread. Surveillance originates in a paradoxical fashion - being the outcome of the quest for citizenship, and also of greater centralized state control - and is experienced with ambivalence. Contemporary surveillance systems are meant to ensure that we are paid correctly or receive appropriate welfare benefits, that terrorism and drug-trafficking are contained, that we are made aware of the latest consumer products, that we can be warned about risks to our health, that we can vote in elections, that we can pay for goods and services with plastic cards rather than with the more cumbersome cash, and so on. Most people regard these accomplishments as contributing positively to the quality of life; hence, the lack of resistance to systems whose advantages seem to carry with them a number of acceptable risks.

On the other hand, while we are both grateful for the protection or procurement of rights which surveillance affords, we are simultaneously irritated and defensive when meddlesome bureaucracy invades what we see as our private space, or angered at the

threats posed to our autonomy. In the late twentieth century, surveillance is expanding in subtle ways, often as the result of processes intended to pursue goals such as efficiency and productivity. Moreover, its subtlety is increased by its present day electronic character. Most surveillance occurs literally out of sight, in the realm of digital signals. And it happens, as we have already seen, not in clandestine, conspirational fashion, but in the commonplace transactions of shopping, voting, phoning, driving, and working. This means that people seldom know that they are subjects of surveillance, or, if they do know, they are unaware how comprehensive others' knowledge about them actually is.

What does this mean for our sense of identity, our life chances, our human rights, our privacy? What are the implications for political power, social control, freedom, and democracy? The answers to these crucial questions draw us into a number of important debates, sometimes in disciplinary areas that are conventionally separate. I list these below, but throughout the dissertation I demonstrate how they must be considered together if we are to properly grasp the dimensions and implications of contemporary surveillance as well as address the two questions raised earlier: why is privacy legislation for the private sector in this country "an idea whose time has come" and how can public awareness about surveillance be increased?

Part I suggests that data protection has become a new social science subfield. As one might imagine, the development of any new subfield is fraught with controversy. No settled views on the origins, character, or likely direction of electronically enabled surveillance are available. However, at the risk of oversimplifying, it is possible to characterize the subfield in terms of three main theoretical perspectives. These

perspectives may be summed up in terms of their leading motifs: capitalism, rationalization, and power. Such perspectives are important in helping us to understand how modern surveillance has been established in different social and historical contexts: government administration, the capitalist work situation, and the consumer marketplace. These contexts are discussed at length in Part I.

In the capitalist perspective, derived primarily from Marxian ideas, the thrust and impetus of surveillance is always connected with the capitalist drive for greater profit. This may be expressed in different ways, from the constant renewal of technologies to facilitate greater degrees of efficiency and productivity, to the exporting of efforts directed at managing production, to more recent attempts to manage consumption. Thus, authors such as Frank Webster and Kevin Robins (1986) speak of "cybernetic capitalism," and Rob Kling and Jonathon Allen of "information capitalism" (1996). In his vast contribution to surveillance studies, Oscar Gandy sees the "global capitalist system" now guided by what he calls the "panoptic sort", which uses new technologies to assign different economic values to different sectors of a given population (1993).

For Karl Marx, surveillance was located within struggles between labour and capital in the business enterprise and the capitalist system. Previous means of co-ordinating workers on a large scale had involved coercion; under capitalism, labour was no longer coerced. According to the new doctrine, the worker was, in a formal sense, free. But the capitalist manager still had to maintain control of workers so that businesses could be kept competitive by producing as much as possible within a given time at the lowest cost.

Hence what we now know as "management" was developed to monitor workers and to ensure their compliance as a disciplined force. The idea of bringing workers together under one roof, in factories and workshops, has often been seen as a way of maximizing technical efficiency, making full use of machinery, and so on. But it can equally well be argued that the use of factories to ensure labour discipline through the oversight of workers' activities was at least as important, if not more so. Marx's recognition of this makes his work vital to an understanding of modern surveillance.

Understanding surveillance from the capitalist perspective makes sense. Clear historical patterns may be traced, and the whole process may be seen as having an economic logic. It also makes possible a critical stance in which systematic inequalities are exposed and a critique is made of the major organizations and ideologies that perpetuate the system. However, in its less sophisticated versions, its shortcomings also relate to these factors. It is all too easy to use capitalism as a catchall explanation, without, for instance, noting ways in which bureaucratic and technical logic themselves may play a relatively independent role. And the critical stance may sometimes lack nuance. Surveillance is not an unmitigated evil, but rather a two-faced social phenomenon with which many cheerfully collude for the sake of advantages that accrue to them. People are willing to sacrifice a little privacy for the sake of political participation or consumer convenience. For these reasons, many communications scholars seeking a framework within which to explain surveillance draw upon a range of perspectives, each of which may contribute some significant insight.

A more Weberian perspective focuses on the processes of rationalization that characterize the development of modern organizations. Max Weber acknowledged the role of surveillance in capitalist enterprises but resisted the restriction of surveillance to the context of class relations. For him, surveillance is bound up with bureaucracy, of which capitalist business enterprises are but one type. Modern organizations are characterized above all by their *rationality*, a feature that both gives them coherence and distinguishes them from previous forms of organization.

In the capitalist workplace, for instance, this rationality entails accounting by means of double entry book-keeping. Everything is geared towards making possible carefully calculated decisions. All administration is based on written documents, processed by a hierarchy of salaried officials, and impersonal rules based on up-to-date technical knowledge. Efficiency is allegedly maximized through this system; but so is social control. Members come to accept the rules as rational, fair, and impartial. The director of a bureaucracy can predict with certainty that orders will be implemented in a rational manner. As Christopher Dandeker says, for Weber, "rational administration is a fusion of knowledge and discipline" (1990: 217).

The Weberian perspective is sometimes - erroneously - associated with a gratuitous emphasis on technical change. Technological developments, expressing the rationalizing motif, are sometimes taken to be central to an understanding of surveillance. Organizational computer power somehow spells "Big Brother". Although a Weberian approach would indeed accent the unique contribution made by specific new technologies, it is a mistake to equate this with a form of technological determinism. Communications

scholars tend to repudiate such a position, but it is not uncommon, especially in many popular accounts, to find new technologies branded as the "cause" of new surveillance practices.

Jumping to the late twentieth century, the work of Michel Foucault points beyond bureaucracy. He places surveillance in the broader context of discipline in society-at-large, not just organizations. Indeed, only since Foucault has surveillance been accorded a central position in social analysis. For Foucault, modern society is itself a "disciplinary society", in which techniques and strategies of power are always present. Though these may originally develop within specific institutions such as armies, prisons, and factories, their influence seeps into the very texture of social life. Power, in this view, is not a possession but a strategy. Power makes for constant tension and struggle as those subjected to it resist it with their own tactics. In modern societies, people are increasingly watched, and their activities documented and classified with a view to creating populations that conform to social norms. The knowledge of what happens is thus intrinsically bound up with power.

Foucault's work has been used in various ways in surveillance studies. First, he notes the apparent similarity in surveillance practices within diverse social spheres, such as the factory, school, and prison. This has raised critical questions about the extent of such commonality, questions on which Weberians have been particularly insistent (Lyon, 1992). Second, Foucault's surveillance theory points up the ways in which surveillance extends into the micropractices of organizations, the "capillary" level, classifying as well as observing subordinates. Third, although Foucault's studies refer primarily to modernity,

some take the phenomenon of electronic surveillance to presage a postmodern condition in which virtual "selves" circulate within networked databases, independent of their Cartesian counterparts who use credit cards and are identified by their social insurance numbers (Clarke, 1994). For example, Mark Poster, whose work best exemplifies the Foucauldian approach, suggests that databases have become the new text in Foucault's sense of discourse (1989 and 1990).

The Foucauldian perspective has advantages and drawbacks. In the modern world, access to information does seem to be increasingly connected with power - especially today, with the availability of cheap and efficient modes of data processing. On the other hand, Foucault's perspective seems to revolve around the concept of power in a way that almost excludes other considerations; power, expressed as domination or violence, is all there is. Little space remains for examining how people actually interact with each other in surveillance situations, still less for approaching these questions from a different standpoint.

My own perspective on surveillance takes account of what Marx, Weber, and Foucault have to say but is not exclusively aligned with any one of them. Instead, I have found help in organizing my explanatory tools from Anthony Giddens. Giddens, as a sympathetic critic of all three theoretical traditions, has attempted to produce an intelligent synthesis of the best of each. His emphasis on surveillance as a modern institution and, from structuration theory, his focus on its enabling as well as constraining features, draw the attention back to human beings as "knowledgeable agents" within surveillance situations. In short, his work provides a useful springboard into surveillance studies,

particularly into concepts of *participation*, *personhood*, and *purposes* which I develop in Chapter Three. These concepts have a crucial relation to social processes of communication.

Thus, I argue that the perspectives outlined by Marx, Weber, and Foucault are less important to the question of which of the three theorists is correct as they are to their overall contribution to contemporary surveillance theory. In this regard, the three traditions have taught us that whether it is an aspect of class relations, or rationality, or a pervasive dimension of society itself, surveillance must be seen as a central feature of modernity. From the earliest days of modernity, administrators collected and recorded personal details of given populations, and capitalist business organizations monitored and supervised employees in order to enhance their efficiency. Increasingly, heavy dependence was placed on the role of knowledge in generating and maintaining power. As such, it is incorrect to think of surveillance as a twentieth-century phenomenon made possible solely by new information technology and the computerization of the so-called post-industrial society. To view surveillance in this light is to elevate technology above its place. We must get away from the zero-sum game of "more technology = less freedom".

To this end, Part I also explores two popular models of surveillance, both of which are rooted in particular technological designs. The first, George Orwell's *Nineteen Eighty-Four*, focuses on electronic media as a chief tool for manipulating the masses through unremitting propaganda. It features Big Brother, who appears on the telescreens of public and private buildings, and claims to monitor everything. Hence "Big Brother is

watching you", which is now one of the most readily recognized catch-phrases in the English language.

The second, which has gained much ground in the analysis of surveillance, is Bentham's Panopticon. Much of the impetus for this comes from the fashionable flurry of Foucault studies that began in the 1980s, but now sufficient empirical work has been done to demonstrate the relevance of at least some aspects of the Panopticon to electronic surveillance. The remainder of Part I is thus taken up with the question of how far Big Brother and the Panopticon provide a useful model for understanding electronic surveillance. In this regard, I argue that while no single model is adequate to the task of summing up what is central to contemporary surveillance, important clues are available in both *Nineteen Eighty-Four* and the Panopticon.

For example, Orwell's nightmare, though technologically rather dated now, correctly spotlights the role of information and technique in orchestrating social control. Its focus on human dignity and on the social divisions of surveillance also remain instructive. But the shift from violent to non-violent methods of social control has come a long way since Orwell, and is given much greater scope by the advent of information technology for surveillance. Moreover, Orwell's vision was dominated by the central state. He never guessed just how significant a decentralized consumerism might become for social control.

The Panopticon, on the other hand, offers scope for social analytic interpretation in precisely such contexts. Studies referred to in Part I illustrate the broad sweep of the Panopticon's potential relevance in diverse areas, from government administration to the

consumer marketplace. The Panopticon points to the role of subordination *via* uncertainty, and to ways in which power pervades social relations. As such, it does seem to hold promise for the age of subtle, computer-based surveillance. Yet its use is also fraught with difficulties. For instance, while the adoption of computers does blur the distinctions between surveillance spheres, and thus poses questions for surveillance theory, this does not mean they are dissolved altogether. The Panopticon offers no neat "total" explanation of surveillance. In addition, the Panopticon as a means of exclusion may well be in eclipse, leaving the advanced societies under the superior sway of consumerism, with only a minor role left for the harsher panoptic regimes. Thus, while it is undeniably illuminating, analysis based on the Panopticon image also retains some serious disadvantages.

Finally, it is worth noting that Orwell's "Big Brother" and Foucault's understanding of the Panopticon should in no sense be thought of as the only, let alone the best, images for yielding clues about surveillance and information technologies. Powerful metaphors lie relatively unexamined in various films as well as in novels such as Franz Kafka's *The Castle* or Margaret Atwood's *The Handmaid's Tale*. In the latter, the gendered dimension of categorization, and its implications for a stunted citizenship for women, is vividly portrayed. At present, however, most surveillance studies are informed by either Orwellian or Foucauldian ideas, which is why it is to these writers that Part I contains most reference.

Thus, the first half of Part I situates electronic surveillance in its historical context with the idea that particular and specific events, such as Minister Manley's announcement

on future privacy legislation for the Canadian private sector, can only be understood when placed against the backdrop of a broader, long-term picture. Following from this, the second half of Part I suggests that the context within which surveillance needs to be rethought is not only the historical - which yields certain clues about why new technologies and policies are shaped in a particular way - but also the theoretical and critical. In this regard, I argue that surveillance theory has benefitted tremendously from social analysis, but in terms of producing a normative theory, difficulties still remain. Regrettably, some of the most telling insights come from theory that emphasizes the negative and that ultimately offers no buffer against paranoia. As an alternative to this, I propose that the social analysis of surveillance be harnessed to a consideration of elements of the "good society" as opposed to those of the "bad", as seen in Orwell's *Nineteen Eighty-Four* and Foucault's Panoptic world. In doing so, we can achieve a clearer understanding of contemporary surveillance as well as seek alternative models of understanding and action.

Part II: Surveillance and Public Policy

Part I describes the larger social and historical background within which Minister Manley's announcement on future privacy legislation is situated. Such a background provides some important answers, mostly in terms of social understanding and long-term historical trends, to the question of why his announcement represents an "idea whose time has come". However, to unearth other answers, which have to do with more specific short-term conditions and events, we must look to Part II of the dissertation. In this

regard, Part II notes that policy analysts often find it useful to distinguish between the background conditions that make policy change possible, and the more immediate events that motivate political decisions (Simeon, 1976).

Part II examines four necessary, but not sufficient, conditions without which Minister Manley probably would not have made his announcement on future privacy legislation: (a) the market implications of inconsistent privacy standards; (b) the economic implications of international standards; (c) public opinion on privacy; and (d) the shifting line between the "public" and "private" sectors. In addition, Part II outlines three proximate events that contributed to the government's announcement: (a) the work of the Canadian Standards Association (CSA) in negotiating a Model Code for the Protection of Personal Information; (b) the work of the Information Highway Advisory Council (IHAC), which recommended a legislative framework for privacy protection in its 1995 report (IHAC, 1995); and (c) the work of the Uniform Law Conference of Canada, which created recommendations for a Uniform Personal Information Protection Act. By examining these background conditions and proximate events, it is possible not only to understand why privacy legislation for the private sector is "an idea whose time has come" in Canada, but also how the form of such legislation may be shaped.

The Background Conditions for Reform

1. The market implications of inconsistent privacy standards

With the enactment in 1993 of Quebec's Bill 68, *An Act Respecting the Protection of Personal Information in The Private Sector*, Quebec became the only jurisdiction in North America to produce comprehensive data protection rules for the private sector. Bill

68 applies fair information principles to all pieces of personal information collected, held, used or distributed by another person, confined mainly to enterprises engaged in an "organized economic activity". Personal data shall be collected from and with the consent of the person concerned, and shall not be communicated, sold, leased or traded without the consent of that same person. The Access to Information Commission in Quebec (CAI), the body established under the 1982 public sector access and privacy law, is responsible for hearing complaints and rendering decisions.

Bill 68 has created three inter-related concerns for enterprises both in Quebec and in other provinces. First, Section 17 of the law states that "every person carrying on an enterprise in Quebec who communications, outside Quebec, information relating to persons residing in Quebec . . . must take reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned". This provision has yet to be enforced, but Bill 68 does give the CAI sufficient powers to prevent an outward transborder data flow if "reasonable steps" have not been taken.

Second, whether or not transborder data flow restrictions are enforced, inconsistent standards are an inconvenience for Canadian business. For businesses that operate in different provinces, the transaction costs of having to deal with different privacy laws and regulations can create uncertainty and confusion. This is a particularly acute problem for provincially regulated industries like insurance and retail. Such enterprises are obliged to grant rights to Quebec consumers that citizens in the rest of the country do not

enjoy. Some businesses have thus harmonized their rules and declared that their practices in the rest of Canada conform to the Quebec standard.

Third, the patchwork can have more direct economic consequences through the unintended creation of an "unlevel playing field" that may put some businesses at a competitive disadvantage. Quebec's Bill 68 only formally covers provincially regulated entities and excludes the financial, telecommunications, and transportation sectors. At the same time, entities in those federally regulated sectors have clients and competitors (such as the insurance industry) that are covered by Bill 68 in Quebec but which are subject to few data protection rules in other provinces.

This is one reason why the extension of the federal Privacy Act to the federally regulated private sector would not produce a comprehensive set of rules for the entire marketplace. Although this option has been advocated in the past (Standing Committee on Justice and Solicitor General, 1987), it would create disadvantages for some sectors over others, and even for some businesses within sectors, such as telecommunications. Federal legislation would not extend to all possible service providers on the information highway, and would create a "patchwork privacy environment in which many market participants would be under no obligation to protect the privacy of their customers" (Stentor, 1994).

The complexity of Canada's patchwork is not only daunting to the privacy analyst, it also creates a significant and increasing set of transaction costs for businesses that operate in different jurisdictions. It is principally for these reasons that the privacy protection issue has risen to the political agenda, and that the rhetoric about "marketplace

rules of the road" and "level playing fields" on the information highway has overshadowed the traditional discourse about human rights and civil liberties within which privacy protection originated. It is also the reason why the lead department in policy formulation is now Industry Canada, rather than Justice Canada.

2. The economic implications of international standards

Foreign jurisdictions acting to harmonize their privacy legislation have also forced Canada to produce a more comprehensive and coherent set of rules. The international agreements of the 1980s, chiefly the Council of Europe Convention and the OECD Guidelines (Council of Europe, 1981; OECD, 1981), have had a negligible impact on personal data practices in Canada. But the recent Directive from the European Union (EU) on the "Protection of Individuals in relation to the Processing of Personal Data" could prove an entirely different prospect for Canadian business (EU, 1995).

The central purpose of this Directive is to harmonize all European data protection legislation to offer common and high levels of protection throughout the EU in order to facilitate trade (Raab and Bennett, 1994). Of particular concern to third countries such as Canada are the concomitant restrictions on transborder data flows outside the Community. The Directive states that the transfer of personal data to a third country is, in principle, allowed only if the third country concerned offers an "adequate" level of protection. In accessing the adequacy of protection, particular account will be taken of the nature of the data, the purpose and duration of the proposed processing operation, general and sectoral data protection legislation, and any professional rules (such as privacy codes of practice) that are "complied with" in the receiving jurisdiction. It is probable that Quebec's Bill 68

will meet the EU standards since the bill was drafted with the EU language in mind. However, the hodge-podge of privacy codes and principles in the rest of Canada will not (Bennett, 1996).

3. Canadian public opinion

It is probable that the government would not have acted had recent public opinion polls failed to demonstrate significant public concern about privacy and support for stronger public policies to protect it. For instance, the 1992 national Canadian public opinion survey *Privacy Revealed* showed that 52 percent of Canadians were extremely concerned about privacy, with 92 percent at least moderately concerned. The report concluded that "There is a pervasive sense that personal privacy is under siege from a range of technological, commercial, and social threats" (Ekos, 1993).

In the Ekos survey, questions were asked about the range of possible policy responses: 80 percent agreed that "when I subscribe to a magazine I feel that they should not sell my name and address to another company"; 83 percent strongly believed that they should be asked for their permission before an organization can pass on information about them to another organization; 71 percent totally agreed that privacy rules should apply to both government and business; and 66 percent believed that government should be working with business to come up with guidelines on privacy protection for the private sector.

When asked to list those institutions about which they are most concerned, the following rank ordering was discovered: (1) companies that sell to people at home; (2) survey companies; (3) telephone companies; (4) retail stores; (5) credit bureaus; (6) cable

companies; (7) insurance companies; (8) banks; (9) government; (10) police; (11) Statistics Canada; (12) employer; and (13) doctors and hospitals. This survey reveals that Canada has so far only regulated the personal information practices of the institutions that are *most* trusted by individual citizens.

4. The shifting line between the "public" and the "private"

Finally, and of particular concern to Canada's small network of privacy and information commissioners, has been the gradual erosion of the boundaries between the "public" and the "private" sectors. This distinction is being eroded by efforts to privatize or hive-off government functions (OPC, 1995). Commissioners thus worry that the protection offered by legislation like the federal Privacy Act are circumvented when "private" organizations perform "public" functions, and require the use of personal data held in public agencies to fulfill those obligations.

Illustrations include: the use of smart cards and automatic teller machines for the dispensing of government benefits; the matching of data on welfare recipients with bank or financial records to ascertain eligibility; the trading of government personal information to enhance revenue; the use of profiling techniques developed by the direct marketing industry to target segments of the population; the use of credit reports for security checks; and so on.

The pervasiveness and flexibility of new information technologies make it increasingly difficult to determine which organizations in which places "hold" personal data. The decentralization, flexibility, and interactivity of the "information highway" is also a constant theme, which leads, therefore, to calls from the Federal Privacy

Commissioner, among others, for some clear and common "rules of the road" (OPC, 1994: 8-10).

The Proximate Causes of Policy Reform

1. The Canadian Standards Association Model Code for the Protection of Personal Information

The confusion over the privacy patchwork, the growing concern about the EU Directive, as well as the desire to avoid regulation, has led stakeholders to seek a more innovative solution to the problem of information privacy under the auspices of the Canadian Standards Association (CSA). Since 1992 a CSA Technical Committee, representing government, industry, and consumer groups, has been updating and revising the OECD Guidelines with reference to the Quebec legislation and the emerging EU Directive. The Model Code for the Protection of Personal Information was passed without any dissenting vote on September 20, 1995, subsequently approved by the Standards Council of Canada, and published in March 1996 as a "National Standard of Canada". The idea originally was for the code to be adopted *voluntarily* by different sectors, adapted to their specific circumstances, and used as a way to promote "privacy friendly" practices. The CSA Model Code is potentially, therefore, a different type of regulatory instrument from the privacy codes passed by many industries (Bennett, 1995). It can provide a greater consistency of policy, more consumer awareness of privacy rights, a better yardstick for the measurement of the adoption of data protection, and a greater level of responsibility for the collection, storage, and disclosure of personal data.

However, the role that the CSA might play in certifying or registering industry codes and practices has not yet been determined. All along, the standards approach has been appealing to privacy advocates because of the potential to register data users (in both the public and private sectors) to the standard and thus to oblige them to implement fair information practices. The scrutiny of operational manuals and/or on-site auditing could be a prerequisite of maintaining a registration (Bennett, 1995).

The major value of the CSA Model Code is that it has been openly negotiated by industry, consumer representatives, and governments. It represents a national consensus on the standards for privacy protection expressed within ten clearly articulated principles: accountability; identifying purposes; consent; limiting collection; limiting use; disclosure and retention; accuracy; safeguards; openness; and individual access and challenging compliance. The substance of a privacy protection policy has thus been brokered. The CSA negotiation constitutes a crucial stage in the development of a national public policy. Future privacy legislation for the Canadian private sector will likely be based upon this standard.

2. The Information Highway Advisory Council

It has been the responsibility of the Information Highway Advisory Council (IHAC) to advise Industry Canada about the multitude of policy issues associated with open access to the information highway. In this regard, a prominent goal from the outset has been to ensure privacy and security. In September 1995, IHAC issued its final report which included a set of recommendations to "ensure privacy protection on the Information

Highway". In addition to encouraging adoption of voluntary standards based on the CSA Model Code, the Advisory Council recommended that the federal government:

> . . . create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA Model Code, while allowing the flexibility to determine how they will refine their own codes.

The establishment of a federal/provincial/territorial working group was also recommended to implement the CSA principles in all jurisdictions.

The significance of IHAC's recommendation lies in the broad support from the *private* sector participants on the council, even though most industrial associations were still publicly supporting self-regulation (Akay, 1995). Subsequently, however, the Canadian Direct Marketing Association became the first industrial group to endorse a legislative approach in its October 1995 call for national legislation based on the CSA standard (CDMA, 1995). It probably did so because it was confident that its members could abide by the CSA standard, and because direct marketers who were non-members would then be forced to play by the same rules. In so doing, the CDMA broke ranks with other private sector associations. This move could prove profoundly important. Any business interest that wishes to oppose legislation must not only argue against privacy commissioners and advocates, it must also now oppose the CDMA.

3. *The Uniform Law Conference of Canada*

In 1995, the Uniform Law Conference of Canada (ULCC) decided that it could play a vital role in the development of future privacy legislation for the Canadian private sector by ensuring a consistency between federal and provincial approaches. It decided to

create a task force to come up with recommendations for a "Uniform Personal Information Protection Act". This consultation took place with private sector, consumer, and government representatives as well as with other data protection experts throughout 1996. A report was published later in that year with the following recommendations: that the ULCC should support the drafting of a uniform statute that could serve as a model for federal and provincial legislation; that such a law should apply to everyone in the private sector regardless of size; that the principles within the CSA Model Code represent a good base upon which to build a uniform statute; and that existing data protection agencies be given mandates for public education, powers to receive complaints, and conduct investigations, mediation, and adjudication. There is thus agreement in the ULCC about basic data protection issues, although it is likely that further analysis and negotiation will be required when the EU Directive comes into effect in October 1998.

The Elements of a Canadian Privacy Policy for the Private Sector

Through an examination of background causes and proximate events, Part II analyses the process by which Canada has moved to the brink of privacy legislation for the private sector. An examination of this process provides some important answers to the question of why such legislation is an "idea whose time has come". To this question, Part II unearths answers which are short-term in nature; that is, they focus on legislation, self-regulatory codes, policy documents, and a social, political, and economic climate that has been shaped by talk of the "information highway" and an "information society". This is in contrast to Part I of the dissertation where surveillance is placed against the backdrop of

modernity in an attempt to outline the broader historical and social context within which privacy legislation has developed.

However, both contexts are important to Minister Manley's announcement. The long term context is important because it highlights a wider comparative picture within which particular events must be situated if we are to fully appreciate their significance. And the short term context is important insofar as Minister Manley would not have made his announcement if prior work on privacy protection had not been done. As we have seen, this work took place in three separate arenas: the Technical Committee of the Canadian Standards Association (CSA), the industry-dominated Information Highway Advisory Council (IHAC), and the Uniform Law Conference of Canada (ULCC). In turn, the work done in these arenas was shaped by four necessary, but not sufficient, background conditions: (a) the potential market consequences of inconsistent privacy standards; (b) the economic implications of international standards; (c) Canadian public opinion; and (d) the shifting line between the public and private sectors.

Finally, as a coda to this cursory glance at short and long term contexts, it is important to ask not only *why* privacy legislation for the private sector is "an idea whose time has come", but also *what form* this legislation will take. In this vein, Part II suggests that the lateness of Canada's response to the privacy issue may be an advantage in that policy makers have had the opportunity to learn from other countries and to fashion a policy response that is perhaps more sensitive to the dynamics and complexities of the information highway. If the government acts on its intentions, then the essential nature of the policy will probably be as follows.

First, Canadian governments will probably be urged to apply the full range of available policy instruments to the problem: self-regulatory codes, legislation, and privacy-protecting technologies, especially public key encryption (Industry Canada, 1994). These are the "policy instruments" within the "tool kit" (Hood, 1986). Second, there have been a greater number of self-regulatory initiatives in Canada than in any other country. Any personal data protection policy will inevitably rely on a significant measure of self-regulation, and will reject onerous licensing and registration regimes. Canada has been creating a data protection regime from the "bottom-up". All commentators recognize that this experience lays an important foundation. This then raises intriguing regulatory questions about the role of privacy codes of practice within a legislated system (Bennett, 1995). Third, and finally, the existence of the CSA standard potentially offers a compliance mechanism that is present nowhere else. When the CSA decides to offer registration or certification to this code, a crucial auditing mechanism will be established that will oblige businesses to develop codes of practice, demonstrate how these codes are implemented, and force regular and independent auditing through an accredited registrar such as the Quality Management Institute (QMI). Registration to the standard would occur under pressure from consumers, clients, and domestic and foreign governments. It may even promote a more effective system of privacy auditing than currently occurs anywhere in the world. Thus, a comprehensive legislative solution to privacy protection in Canada would integrate the existing mechanisms of industry and company codes, the CSA standard, and the Offices of the federal and provincial privacy commissioners. As such, it would constitute a "mosaic of solutions" (Cavoukian and Tapscott, 1995).

Part III: Challenging Surveillance

There is, however, an important ingredient missing from this mosaic: public awareness and involvement, an idea which finds frequent mention in privacy scholarship (Gandy, 1993 and Bennett, 1996). In this vein, Part III suggests that two kinds of responses to surveillance have emerged over the past few decades. These may be divided into *technical* responses, those that seek legal or technological means or the restriction or addition of security features to surveillance systems, and *mobilization* responses, which seek to organize opinion or opposition to surveillance. Examples of the former would include the passing of laws regarding data protection and privacy, while examples of the latter would be the activities of civil rights or consumer groups that attempt by legal, lobbying or other activities to protest or limit the spread of surveillance. It is important to note that the activities and ambitions of these two responses to surveillance overlap. For example, the mobilization of opinion may lead to changes in the law. As such, technical and mobilization challenges to surveillance should be viewed as two ends of a continuum, with resigned acceptance at one end, and fundamental opposition at the other.

In addition, Part III suggests that modern societies are almost by definition preoccupied with problem-solving. That is to say, it is a condition of modernity that societies become increasingly aware of themselves through the processes of management, planning, and so on. The logic of technological and bureaucratic development frequently proceeds on the assumption that problems created by them are in principle solvable by them. Surveillance is no exception. For instance, Part III observes that if technological advancement produces perceived problems, then it is often believed that some

technological fix - such as encryption or enhanced security - or legal remedy - such as data protection or privacy law - can be applied to overcome it. This kind of solution basically accepts the *status quo* while acknowledging that improvements are always desirable. Another kind of approach is much more doubtful about the *status quo*, and is visible through an analysis of social movements.

Part III notes that an understanding of the dynamics of social institutions in the modern world - capitalism, industrialism, the nation-state, and militarism - has led some theorists to expect to see social movements generated in opposition to those institutions. Indeed, over the past two decades theorists have argued strongly that the more conventional politics of modern societies is being challenged by social movements, whose concerns transcend traditional debates resting on class, nation, and so on (Melucci, 1989). But while the opposition of Green movements to industrialism or peace movements to militarism may appear to echo the more venerable and historically longer term labour movements' resistance to capitalism, it is far from clear that surveillance has generated much by way of systematic opposition in terms of identifiable social movements, though there are signs that this may be changing. Part III examines the status and achievements of such groups and movements (Giddens, 1985; Melucci, 1989), and also offers possible reasons for their relative absence or weakness.

Finally, because of the sparse information on awareness movements in the privacy literature, Part III examines the growth of a successful awareness movement in another field: breast cancer. In this vein, it suggests that there are some interesting cross-sector parallels between the objectives of the breast cancer awareness movement and those of the

privacy awareness movement. For instance, both movements are concerned with the problem of increasing public awareness and involvement without relapsing into the paranoid. In addition, the two movements have struggled to overcome "minority" perceptions; in the case of breast cancer, that it is a "woman's" disease and, in the case of surveillance, that individuals claiming privacy invasions from new information technologies represent the exception rather than the norm (Regan, 1995). Finally, both movements have developed an extensive and growing presence on the Internet as a means of attaining their respective objectives. Part III comments on these parallels as well as examines important differences between these movements with respect to three social processes: definitional reconstruction of issues; pressure group organization; and media use. It is hoped that from this cross-sector analysis privacy advocates and scholars may be able to do some "lesson-drawing" (Bennett, 1990) for their own pursuits in raising public consciousness about surveillance.

Methods of Analysis and Data

Typically, there are two routes "into" surveillance studies. The first is from the social analysis of surveillance, work, and the state, and the second is from the political analysis of or direct engagement with surveillance and public policy, particularly as it is expressed in the discourse on "privacy". Both of these routes have their own methods of analysis and data, which will be visible in different parts of the dissertation. In Part I, my discussion of surveillance resembles the first route into surveillance studies. Generally, this route is concerned with developing theoretical and critical models through which

surveillance can be understood. As such, Part I outlines my perspective on surveillance, taking into account what the three major traditions in surveillance studies have to say - the Marxian, Weberian, and Foucauldian. However, I do not exclusively align myself with any one of these traditions and instead argue that the long term solution to the problems of surveillance lies in the areas of *participation*, *personhood*, and *purposes*. From "participation" derive some alternatives to the exclusionary power of surveillance, from "personhood" some criteria by which to judge the data-image, and from "purposes" an antidote to the self-augmenting development of surveillance technologies. These three categories are offered in the dissertation as a contribution to finding direction for hope in a social field dominated by dystopic images such as Big Brother or Foucault's fatalistic Panopticon.

In addition, the former route into surveillance studies is concerned with rethinking the historical context within which surveillance has developed. In this regard, Part I examines surveillance as a central dimension of modernity, an institution in its own right, not reducible to capitalism, the nation-state or even bureaucracy. As such, Part I shows that surveillance has more than one face: it simultaneously represents both a means of social control *and* a means of ensuring that citizens' rights are protected. This historical understanding of the two faces of surveillance yields important clues as to why public policies are shaped in a particular way. For example, we may be tracked by our Social Insurance Number but the same computerized system also ensures that we receive unemployment benefits; any future privacy legislation for the private sector in Canada will probably reflect this duality. In other words, it will probably attempt to balance threats to

individual privacy against increasing consumer demand for the provision of goods and services via the information highway and other electronic channels. As such, it will reflect the historical development of surveillance as both a constraining *and* enabling force.

Finally, the data used in Part I also resemble the data used by many social theorists. I draw on illustrative material from a variety of sources rather than attempt to paint an exhaustive empirical picture. As such, I use cases to demonstrate important points. These are drawn from the areas of: government administration; the capitalist work situation; and the consumer marketplace. Wherever possible, I make clear where further empirical details may be discovered, but my aim in this section is to place current debates about surveillance in the contexts of social theory and historical developments, not to conduct a systematic empirical study on information technologies and social control. Thus, most of the evidence in this section is based upon selected secondary research materials.

The "other route" into surveillance studies, apart from social analysis, is from the political analysis of, or direct engagement with, public policy, above all as it is expressed in the discourse on "privacy". Rather than situating surveillance in various contexts - historical, theoretical, critical - this route examines actual trends taking place in society today. In particular, it focuses on concerns for what is termed in North America *privacy* and in Europe *data protection*. These concerns have grown steadily since the 1970s, and are manifest in laws, commissions, and conventions in nearly all the advanced industrialized states. Such legal provisions attempt - largely unsuccessfully - to keep pace

with technological advances in data processing and with the symbiotic growth of surveillance practices in government and commercial settings.

Parts II and III of the dissertation use this route into surveillance studies to document the specific ways in which privacy serves as a mobilizing concept to express real social anxieties and fears. In Part II, current privacy laws and privacy codes of practices are examined as well as the background conditions and proximate events that are making policy reform in the private sector possible by the turn of the century. In Part III, concern with the direct political implications of increasing levels of surveillance are examined in the form of awareness movements. Evidence for these two sections is drawn from data commonly used by policy analysts: legislation, government reports and discussion papers, national public opinion surveys, policy documents from privacy stakeholders including industry and consumer groups, and telephone interviews with policy makers and activists. Unlike the data used in Part I, the evidence for Parts II and III is based upon both primary and secondary research materials.

I have chosen to use both routes "into" surveillance studies in my dissertation because surveillance has become a central feature of contemporary advanced societies. As such, contributions are required from both those engaged in social analysis *and* those struggling directly with surveillance realities in the political arena. The social scientists need the jolt of real-world situations and of technological advances to hone their theories such that they connect with what is actually happening, and policy makers and legal experts need the broader, long-term picture in order to make sense of the particular and specific. This is why the dissertation is divided into distinct, but overlapping, sections. It

is hoped that from these contrasting, but complementary positions, the social, historical, and political meanings of surveillance can be analysed thereby leading us to more just, fair, and responsible models of understanding and action for the future.

PART I

Chapter Two: Situating Surveillance Historically

Situating Surveillance: Surveillance and Modernity

Surveillance - literally, some people "watching over" others - is not new. Since time immemorial, people have watched over others to check what they are up to, to monitor their progress, to organize them or to care for them. For example, the rulers of ancient civilizations, such as Egypt, kept population records for purposes such as taxation, military service, and immigration. And the Book of Numbers records how even the nomadic people of Israel undertook a census to record population details as far back as the fifteenth century BC. However, in the late twentieth century, surveillance has adopted a new medium - electronic technologies. Suddenly, the talk is of a "new surveillance", qualitatively different from that which existed before.

For instance, organizations using information technology for surveillance purposes are now able to obtain a detailed picture of the ongoing, everyday lives of individual people with relative ease. Data referring to matters such as financial standing, health records, consumer preferences, telephone transactions, welfare eligibility, residence, nationality and ethic background, educational experience, and criminal activities are readily available in ways that go far beyond what was possible using manual systems of surveillance. Thus, surveillance capacity is augmented by the use of new technologies.

However, it remains to be seen whether or not the introduction of electronic technologies actually portends a "new" surveillance situation. Perhaps surveillance, rather than being a novel phenomenon, has simply undergone a change in character. For example, there are clear parallels between the modern census and the Israelite Census mentioned above, which recorded people's names, ages, and clans, thereby allowing

leaders to calculate how many were suitable for fighting and what land would be required where. This chapter examines these kinds of historical parallels. In particular, it analyses the different contexts within which modern surveillance has been established - government administration, the capitalist work situation, and the consumer marketplace - and it argues that by examining the various trends that have characterized the growth of surveillance in these contexts, it is possible to discover which of those trends is magnified and which diminished by virtue of adopting information technologies. In other words, the historical backdrop to the "dossier society" (Laudon, 1986) is outlined and investigated in this chapter. In doing so, I suggest that we are in a much better position to assess just how far information technology makes a difference to the practices and experiences of surveillance within different organizational settings.

In addition to assessing how enhanced technical power contributes to the intensification of surveillance in various spheres, the historical perspective is important for another reason. By examining the different contexts within which modern surveillance has been established, it is possible to see that today's surveillance systems are historically constituted and are thus the outcome of choices, struggles, beliefs, and aspirations of the past. As such, recent high-tech pronouncements, wrapped in the language of "computers controlling you", simply will not do. While electronic technologies undoubtedly facilitate a massive augmentation of surveillance capacity, there is not some kind of technological determinism at work. It is easy but misleading to exaggerate the social consequences of computers. New technology does have an impact, but it is an impact mediated by broader economic, political, and cultural processes already existing in each modern society. Thus,

rethinking surveillance from a historical perspective reminds us that new public policies, such as Minister Manley's announcement on future privacy legislation for the private sector, are intended not only to respond to recent privacy fears over electronic technology, but also to larger political and economic conditions such as global recession, political realignments following the end of the Cold War, and the growth of high technology industries in countries of the Pacific rim. This is reflected in Industry Canada's announcement that pending privacy legislation is part of a "larger action plan that is intended to ensure that the enormous enabling power of Canada's Information Highway can be harnessed to *create jobs* and *open up new realms of economic possibility and competitiveness for Canadian firms*, small and large, in every sector of the Canadian economy" (Industry Canada, 1996: 2; my italics).

The Nation-State and Modern Surveillance

During the nineteenth century, burgeoning nation-states undertook a series of administrative tasks which were increasingly organized on a bureaucratic basis. For Weber, the growth of these administrative tasks was made possible by the development of a money economy, which provided the means of paying for salaried officials. The kinds of administrative tasks that mushroomed in the nineteenth century include the collection of taxes and other dues, the registration of property, and, later, vital statistical details of births, marriages, and deaths, all of which had to be gathered in a uniform and consistent manner. As the franchise was extended, Weber argues that the range of administrative tasks increased. For example, eligible voters had to be listed for election purposes,

conscripts or volunteers had to be called up when war was declared, and so on. Indeed, the development of one task led to another in order to complete "the jigsaw of bureaucratic advantage" (Lyon, 1988: 30). Bureaucracy appeared to have a life of its own.

Consider, for example, life in Kingston, Ontario in the 1840s. For a brief period of three years, Kingston was the capital of Eastern and Western Canada, but this was a decisive time for the establishment of the modern nation-state. Alexander Galt, Canadian Minister of Finance, pointed out that (Hodgett, 1956: 5):

> Our population, annually increased by immigration, compels more extended arrangements for the administration of justice and the wants of civil government. Our infant enterprises need to be fostered by the aid of public funds and our great public resources nurtured and expanded by the erection of public buildings.

Among the administrative tasks facing a young Canada - not yet a full nation-state - were recording property transactions, caring for the native population, regulating fishing, licencing and collecting dues for lumbering, passing immigrants up the waterways to the interior, as well as providing government services for transport and communication, roads, bridges, canals, ports, taxation, and customs and excise.

From 1841, under the supervision of Lord Sydenham, the various administrative services were rationalized into distinct departments, each with its own head. Administration, finance, defence, education and welfare, natural resources and development; each found its place within the overall scheme. In short, the seeds of modern bureaucracy in Canada were sown at this time. The main outlines of modern administration, still largely recognisable today, took shape.

These, then, are the kinds of administrative tasks undertaken by the burgeoning nation-state during the nineteenth century. It is possible to observe how such tasks were bureaucratically organized as well as how they contributed to the rise of surveillance insofar as most of them involved personal documentation. But it is also noteworthy that the nascent "surveillance society" described here has more than one face. It may be viewed from the perspective of social control or from that of social participation. The administrative machinery constructed during the nineteenth century can be understood both as a negative phenomenon - Weber's "iron cage" of bureaucratic rationality or Foucault's "disciplinary society" - or, more positively, as a means of ensuring that equal treatment is meted out to all citizens. It is a mistake to focus exclusively on one face of surveillance.

Finally, the burgeoning nation-state differed from earlier, more traditional ones in at least one crucial respect; means other than direct violence were increasingly sought to contain disorder. As agricultural land was enclosed for larger scale use, and newly landless labourers sought employment in the cities and relief in the parish, constant fears were expressed about the potential for unrest. But the means used to ensure order involved progressively more use of the separation - or "sequestering" as Foucault has it - of populations who deviated from the desired norms of "society". In Britain and elsewhere, the workhouse, the hospital, and the prison served as places where the disobedient or the deviant could be "put away" or "reformed" into constructive citizens. In this way, institutions like prisons could become not only places of punishment but also

places where ideals were upheld and realized. The vision of order over and against potential chaos could be maintained and even exemplified in prisons.

Something similar may be said for the city, although some doubt exists as to how far the apparently rational schemes of the urban planner really did contribute to the public good. Stanley Cohen's account of Lewis Mumford on the city is instructive here (Cohen, 1985: 210):

> The dark shadow of the good city is the collective human machine: the dehumanized routine and suppression of autonomy, first imposed by the despotic monarch and the army, is now the 'invisible machine' of the modern technocratic state . . . Mumford described how the utopian ideal of total control from above and absolute obedience below had never passed out of existence, but was reassembled in a different form after kingship by divine right was defeated.

From the nineteenth century onwards, city planners began to take note of the internal social control function that cities could display. Policing took place in city streets, the location of possible criminality and unrest. Law and order were pursued at once architecturally and through rational planning, strategically. Embryonic forms of street surveillance within the "urban fortress" began life well before the era of wall-mounted surveillance cameras.

The other face of surveillance has to do with social participation or "citizenship". Just after the Second World War - the experience of which stimulated much transition from the "warfare" to the "welfare" state - T.H. Marshall published a small classic on *Citizenship and Social Class* (1950). He argued that modern welfare systems "abate" the worst effects of capitalist inequalities and are an outcome of citizenship. Earlier citizenship gains are the foundation on which welfare states are built. According to

Marshall, civil rights emerged first, having to do with individual liberty and equality before the law. Subsequently, political rights developed in the form of widening franchise and the right to seek political office. The third, "social rights", are somewhat vaguely defined, but comprise, for Marshall, "a modicum of economic welfare and security" and the "the right to share in the full heritage and life of a civilized being according to the standards prevailing in society" (1950: 11).

From this point of view, the surveillance systems of advanced bureaucratic nation-states are not so much the repressive machines that pessimists imply, but the outcome of aspiration and strivings for citizenship. If government departments are to treat people equally, which is the starting point for the first of Marshall's rights, and from which other rights follow, then those people must be individually identified. For example, to exercise the right to vote, one's name must appear on the electoral roll; to claim welfare benefits, personal details must be documented, and so on. Thus, as Nicholas Abercrombie and others insist, the individuation that treats people in their own right, rather than merely as members of families or communities, means freedom from specific constraints but also greater opportunities for surveillance and control on the part of a centralized state (1986).

The Marshall account of citizenship rights has been criticized on several counts, one of which is that the process of establishing "rights" took place in different ways in different countries and thus cannot be extended beyond Marshall's England. In the United States, for example, democratic participation extended only slowly beyond the confines of a white, male, landowning elite. Blacks in some southern states continued to be excluded by means of poll-taxes and literacy requirements up until the civil rights movement and

subsequent court action in the 1960s. However, the essential point of discussing Marshall stands; modern surveillance is simultaneously a means of social control *and* of guaranteeing rights of social participation. Surveillance has two faces.

The rise of the "surveillance society", then, is inextricably bound up with the growth of the modern nation-state. As the range of necessary administrative tasks expanded, bureaucratic organization evolved as a means of co-ordinating activities. People's daily lives were thus increasingly subject to documentation within all-encompassing files of the bureaucratic state. All this may be seen from two perspectives: as an attempt to impose new forms of order, to control situations that threatened to breakdown into chaos as the now-familiar urban-industrial world came into being, and as the result of the quest for full citizenship and democratic participation in the new order, which required for fair treatment that individuals be identified, registered, and documented in proliferating dossiers.

Today, it must be asked whether the late twentieth century use of information technology portends further alterations in state power. Certainly, we have seen from the historical rise of the modern nation-state that surveillance concerns the control of information, which is why computer power is significant. But the question, of course, is in what ways is it significant? New electronic technologies have made possible a massive expansion of information storage capacity and processing potential. Applied to the business of personal information, this enhanced capacity has major implications for surveillance. For example, integrated profiles of individual citizens have become increasingly available. In addition, records can now be retrieved and compared with

astonishing ease. This is true not only within the organization that originally collected the data, but between organizations that are both geographically and functionally remote.

In the United States, for instance, a bizarre case concerns Farrell's Ice Cream Parlour, which sold the name-list of those claiming free sundaes on their birthdays to a marketing firm. Soon after, the ice cream eaters were surprised to find draft registration warnings in their mail. The marketing company had sold their details to Selective Service System, who had in turn sold them to the Department of Defence. Thus, the practice of integrating computer networks may facilitate a certain functional convergence between government administration on the one hand and capitalist operations on the other.

But the introduction of computers alone does not account for the creation of a surveillance society. For example, Michael Rubin suggests that the "forces of change" behind the recent massive expansion of administrative surveillance in the United States boils down to one factor: "money" (1988). Though this is not hyperbole, it may be misleading. It might be more accurate to use the term "profit", which indicates how social relations are implicated. Undeniably though, fiscal preoccupations characterize the modern state. This means that, with an acceleration in the pace and size of financial transactions, limitations on the risks involved are increasingly sought.

During the 1980s, for example, the political preference for monetarist policies and their balanced budgets contributed to the search for better methods of control. The impact of this was felt earliest and most keenly within the United States Internal Revenue Service, where new methods of computer matching were utilized to try to contain tax evasion. The direct results were not impressive, although in the longer term the effect was

to contribute to the institutionalizing of such methods. Their matches compared tax returns with reported income files, an activity which aroused considerable ire on the part of taxpayers. Indeed, Rubin observes that the "computer dragnet of the two-thirds population that had taxable income under $20,000 would be very hard-pressed to detect enough tax cheating to reduce the federal budget by as much as one per cent" (1988: 38).

Parallel with this development is the renewed attention paid to the verification of "transfer payments", that is, of the redistributive systems that provide welfare payments and social security to those unable to maintain their position in the consumer marketplace. In the United States, social security expenditure rose from one-half of one per cent of the 1946 federal budget to over twenty per cent in 1996. Medicare, Supplementary Security Income, and Food Stamps have displayed a similar growth curve. With the economic recession of the 1980s and 1990s, and its associated job losses, welfare systems at both national and local levels have been financially stretched, so that any means of rooting out fraud or checking expenditure levels have been welcomed by those charged with operating such systems. Indeed, it seems that greater energy has been expended here than in attempting to establish a fairer system. Surveillance efforts have been redoubled as the price of state welfare.

Alongside the drive for fiscal control, another tendency is discernible; the search for quality control within organizations, not least those involved in government administration. Quality control depends on traceability and is best known from the productive context. To take a trivial example, when I complained to the makers of a muffin mix that my breakfast had been rather flat, they could immediately tell from the

barcoded serial that the offending mix had lain on the shelves for too long. Applied to any kind of personal services, traceability is still crucial to quality control. So-called relational databases are used to link bits of data back to a specific individual, much as the tiny serial found in the wreckage of the plane that crashed over Lockerbie, Scotland located its bombers. Unique identifiers for individuals are being sought more and more in the quest for better quality control, which in turn spells more surveillance.

All these examples show that information technology is implicated in the rise of the contemporary nation-state, for example, in the establishment of computer matching programs and the drive for quality control within organizations. The question of whether such technology actually portends a "new" surveillance situation, however, still remains. In this regard, Gary Marx lists ten characteristics of the new surveillance that set it apart from traditional forms of social control. It transcends distance, darkness, and physical barriers. It transcends time, and this can be seen especially in the storage and retrieval capacity of computers; personal information can be "freeze-dried", to use Goodwin and Humphrey's term (1982). It is of low visibility or invisible; data-subjects are decreasingly aware of it. It is frequently involuntary with prevention being a major concern; think, for example, of bar-coded library books or shopping mall surveillance cameras which are there to prevent loss, not to teach the immorality of theft. It is capital rather than labour intensive, which makes it more and more economically attractive. It involves decentralized self-policing, thereby triggering a shift from identifying specific suspects to categorical suspicion. And finally, it is both more intensive and extensive, or, to use Stanley Cohen's metaphor, the net is more pliable and wider (1985).

Marx's arguments lead me to conclude that new technology - specifically information technology - does indeed make a difference. Simply put, information technology enables many other processes to work, and tasks to be performed. However, understanding this difference involves some careful thinking, and this is where Marx's view of computer power and surveillance has much to commend it. It does not suggest that technology on its own is capable of some mysterious "effects", nor does it allow us to imagine that all can be explained by reference to the kinds of organizations the technologies serve. Marx resists the stance that we are merely the hapless victims of technological determinism, but his work also implies that we are not hapless victims of social forces either.

This thinking supports the argument that technology should be viewed as an *activity* that has social, political, economic, and cultural dimensions. Seen in this way, as something that is done, technology may be understood both in the technical dimension of what tasks can be done using this or that artefact or system, and in the dimension of social origins and consequences. This is important for Minister Manley's announcement on future privacy legislation for the private sector because it is possible to see how state decisions about new information technology relate to larger, fiscal (corporate) concerns over electronic commerce. For instance, Industry Canada has stated that "failure to seize the opportunity of using Canada's Information Highway will result in reduced competitiveness and the loss of high-growth knowledge industries and high-quality jobs" (1996: 3). Hence, the "time has come" for the state to launch "major policy initiatives and

regulatory overhauls to encourage the construction of the Information Highway" (1996: 3), as well as the necessary legislation to protect privacy on that Highway.

Capitalism and Modern Surveillance

A familiar starting point for the analysis of surveillance within the capitalist workplace is the work of Karl Marx. He realised that locating workers under one roof was a key means of keeping control. He also anticipated that new technologies would be developed to maintain that control, quoting Andrew Ure to make his point: the self-acting mule was "a creation destined to restore order among the industrious classes . . . when capital enlists science into her service, the refractory hand of labour will always be taught docility" (1976: 436). In the later twentieth century, Harry Braverman revived Marx's account and attempted to bring it up to date with reference to new technology, arguing that capital constantly subordinates labour through a division between "conception" and "execution" of labour. In other words, capitalism encourages control by those "in the know" over those who merely carry out predetermined tasks. According to Braverman, the latter thus become a de-skilled and increasingly homogeneous group (1974).

For Max Weber, on the other hand, the process of bureaucratic surveillance in the workplace had as much to do with the socially distinct impetus to rationalize production as with control by a capitalist class. If bureaucratic social organization proved itself technically superior to other means of discipline, it was likely to be adopted in situations of growing competition. Organizational imperatives were at work, according to Weber, that pointed logically to the "visible hand" of management supervision as the most efficient

way of shaping economic life (1978). A hierarchical bureaucracy allows managers to predict, from a knowledge of files, that their wishes will be carried out. Knowledge and discipline are thus fused (Dandeker, 1990).

Going beyond bureaucracy, Michel Foucault argued that surveillance in the capitalist workplace is just one instance of the rise of the kind of disciplinary society that characterizes the modern world. The timing and spacing of human activity is a prime means of regulating social life. Power and knowledge are chronically wrapped together. The Panopticon, which was elaborated by Bentham as prison architecture, not only derived but, for Foucault, reappeared in the capitalist factory. The very architecture of the workshop made workers highly visible and thus amenable to attempts at complete control by their supervisors. In this perspective, however, if "techniques of power are invented to meet the demands of production" then such "production can include the production of destruction, as with the army" (Foucault, 1980: 161).

Elements of the Marxian, Weberian, and Focauldian accounts of surveillance in early capitalism help illuminate what occurred as the discipline of management came into being. The capitalist system introduced new ways of disciplining workers who, in traditional societies, had often enjoyed a far greater degree of control over their labour. Where workers had previously been under the sway of a landowner or other employer, physical forms of coercion were available to deal with recalcitrance. Feudalism did involve force. But when it was accepted that workers had a right to dispose of their labour-power as they chose, however circumscribed that choice may turn out to be, other means had to be found of keeping people at work. One, of course, was sheer necessity;

the need to survive with no other visible means of support but what an employer might give in a pay packet. The other was surveillance, through the timing, placing, and checking of work, seen above all in the factory.

The contrast between working life in traditional societies and in modern capitalist-industrial societies is also illuminated by considering time and daily routines. Whereas in settings that are primarily agrarian daily routines are constrained by season, daylight, and tide, modern work routines are geared to the clock. As E.P. Thompson says in a now-classic article, milking cows, shearing sheep, ploughing fields, fishing, spinning, and weaving are activities governed largely by "natural" forces. These older rhythms of labour are replaced by the "clock-work" routines of the factory and workshop within industrial capitalism (1967). For Thompson, the accent is on time as a commodity; this gives it its specially capitalist flavour.

The new clock-bound routines and reliance on management rather than force were major contributions of industrial capitalism to modernity. Control persisted, of course, but it was a control mediated more psychologically than physically. This "demilitarization" of production is one component of the more general process of "internal pacification" taking place within early modern societies. It connects capitalist practice with the use of prisons rather than brutal and public punishments, with policing rather than the use of the militia for the maintenance of law and order, and with the general growth of the administrative state. In each case, moreover, surveillance activities become a more significant aspect of power relations, but not merely in the sense that the power of capital is enhanced. Closer

surveillance could also ensure that workers were protected from unfair accusation and rewarded for appropriate work.

What remains unclear in this account is just how far the asymmetrical class relations between capital and labour actually define surveillance. A Marx-Weber tension remains at this point (Dandeker, 1990). This tension is not unimportant because, as subsequent discussions show, the character of surveillance has rather different connotations in the hands of Marxists or Weberians. The question boils down to whether surveillance power operates along the axis of class relations, or in relation to bureaucratic divisions, including those relating to occupation and employment. Another possibility, introduced by Foucault, is that power is ubiquitous, operating both at the two levels just mentioned and at every other micro- and macro-level of society.

Undoubtedly modern capitalist surveillance induced a crisis of control. As Marx rightly concluded, struggle is built into the capitalist labour contract. Workers resist the imposition of new disciplines and regimes that remove their autonomy and responsibility within the workplace. However, their struggle to regain some control is expressed within the labour movement and trade unions, which have succeeded in securing many rights during the twentieth century.

At this point we should recall Marshall's three-stage schema of citizenship rights. Giddens would modify this by saying that Marshall underplayed the role of "economic rights" in his discussion of how "citizenship" has "abated class struggle" in modern times (1985: 201). Giddens claims that the economic element of citizenship, seen in labour unions and in legislation supporting workers' rights, is "double-edged". It may be seen

both in relation to surveillance and the control of subordinate classes, *and* as a lever of struggle to counter that control. Surveillance, in other words, is again shown to be more complex than a purely Marxist - class power - reading might expect.

While Giddens' comments are in some ways a timely corrective, it is also worth pointing out that *social* rights, so important to Marshall, seem to have been absorbed into Giddens' *economic* rights. Yet they too exhibit the "double-edged" character of surveillance systems. Welfare benefits, for example, may be claimed to alleviate poverty, but at the price of "prying" social workers. Perhaps the problem lies in too narrow a definition of these spheres of surveillance and of citizenship rights.

All this is important background to more recent discussions of surveillance. The theoretical position one takes is closely connected with political possibilities for change. For example, whereas Marx was fairly sanguine about the chances of a revolutionary transformation that would restore autonomy and dignity to workers, Weber was anything but. He warned that "the dictatorship of the official is on the advance", and that this would be true even where the reins of state control might be taken over in the name of socialism. As for Foucault, I argue in Chapter Three that it is even harder in his work to discern anything but negative conclusions about surveillance and control. For him, any dreams of a democratic future seem foreclosed by ubiquitous power.

Putting pessimism on one side for a moment, it is a crucial message of this dissertation that things have changed. In this chapter I look at the growth of surveillance as an inescapable dimension of modernity. But in the closing years of the twentieth century it is abundantly clear that the character of capitalism is altering, as is its relation

with the nation-state. Marx's original insights applied to the liberal era of Victorian capitalism. Since then, capitalism has become increasingly organized, and its activities articulated with those of the nation-state.

The liberal state facilitated capitalism with laws of property and contract and by providing checks on currency and monopoly (Habermas, 1976). But in the middle of this century, capitalism maintained a closer relation with the state, which for a while diminished market forces through the intervention of bureaucratic administration. This galvanized the growth of surveillance practices, especially within large-scale business enterprises. By the 1980s, however, it became evident that another change was in train, variously conceived as "restructuring" or "disorganized capitalism". Scott Lash and John Urry, for example, trace what they claim is a reversal of bureaucratic and centralizing tendencies; hence "disorganized capitalism" (1987). Christopher Dandeker, on the other hand, for whom bureaucracy and surveillance seem inescapably linked, prefers the term "reorganized capitalism" (1990). What does this mean for surveillance?

It is doubtful whether the reorganization or disorganization of capitalism spells the end of surveillance. What we can say is that new styles of management are progressively more bound up with the use of new technologies and that employees are subjected to intensified forms of surveillance. For instance, workers typically find themselves more watched, not just by managers but by workmates and, in a sense, by themselves. However, this does not necessarily entail greater control of workers by management, or mean that new technologies render particular groups less powerful, still less that information technology is deployed in order to subordinate the workforce or that it has a

determining effect on social relations. But it does seem to help maintain the position of capital within the workplace, keeping the basically unequal relations between it and labour in place when older methods of management have started to fail. But to see it in this light is to miss its broader significance.

New technology does not itself produce new social relations nor does it simply reflect or reproduce old ones. This is the error of an easy equation between surveillance by computers and a sort of neo-Taylorism. In many post-Fordist contexts, surveillance transcends traditional Taylorism. For example, Toyota car production does not assume that management has or should have a monopoly of information needed for constant innovation. Toyota dispenses with de-skilling because producing quality goods depends on multi-skilled manual workers. On the other hand, this may mean that fewer workers are required for a given productive process, so that other problems - unemployment - are obscured. So while computers are certainly used for control, this often means control of processes rather than people.

Moreover, in both administrative and economic spheres surveillance is increasingly globalized. This process, facilitated by the rapid deployment of electronic information and communication technologies, has fascinating and significant ramifications. Administrative surveillance, which once occurred predominantly within the borders of the nation-state, now spills over old territorial boundaries, most obviously in the form of international intelligence networks. Commercial surveillance, similarly, forgets frontiers when data on consumers is sought in the global marketplace. At the same time, the emergence of countervailing forces is simultaneously globalized. Data protection in one country

becomes the model for (or in certain circumstances is imposed upon) another country,[2] while social groups concerned with privacy also mount more international operations.

In a post-Fordist context, surveillance touches not only traditional sites of productive activity, but offices and informal situations like restaurants and taxi-cab companies. No occupation, it seems, is immune from surveillance when computer technology is at work, and the significance of this should not be understated. The space-binding capacity of electronic technologies even diminishes the significance of the location where the work occurs. On the other hand, the danger of accounts that begin with new technology and proceed to detail its supposed impacts is that social analysis is effectively abandoned in favour of high-tech journalism. This spawns a lopsided emphasis on the novelty and capacity of new gizmos and gadgets, which may then jump straight to questions either of how you too may take advantage of this advanced computer-power, or of legal or other limits to technology, depending on the perspective taken.

In order to understand social relations, old and new, in the capitalist workplace we must start by recalling the centrality of surveillance to capitalist techniques; how indeed capitalist surveillance forms one of two dominant threads in the tapestry of modern surveillance systems. At the same time, it is clear from the empirical evidence that surveillance involving new technology cannot be reduced simplistically to operations of capital. While in some ways, it may express capitalist relations, the surveillance consequences of new technology are often unintended. Finally, we must ask what kinds of challenge, in terms of surveillance and social control, are thrown up by post-Fordist times.

---

[2] See Chapter Five.

Economic restructuring, and the use of new technologies in particular, make it less and less plausible to think of surveillance simply as a reflex of capitalism. Instead, it seems that the challenge of surveillance appears in its own right. Thus, surveillance is a mode of power mediation which, while displaying some traits amenable to analysis in terms of Marx's class-conflict society or Foucault's "disciplinary society", may not be reduced to either one of them.

The Consumer Marketplace and Modern Surveillance

Commercial, or consumer, surveillance is clearly part of the strategy of capitalist enterprises. But, to date, little social analysis of commercial surveillance exists. What there is commonly starts by seeing it as an extension of other kinds of capitalist surveillance, conventionally associated with the workplace. This putative extension is referred to under various headings, one of which is the term "social management". Vincent Mosco, among others, uses this idea and he makes two important suggestions; one, that surveillance stretches more broadly and more deeply by means of electronic information services and transactions in the commercial sphere; and two, that the consequences of this go far beyond what can be grasped in terms of a "threat to privacy" (1989). For Mosco, such commercial surveillance is intrinsically bound up with social control. I agree. But what exactly are its mechanisms? Is consumer surveillance an extension of modern management techniques, or is it part of a different social order, that in which consumerism is central? Beyond this, is surveillance only about social control?

Mosco's is not a straightforwardly Marxist account of the ways that the management motif has spilled out of the factory and into the home. Mosco hints that more than Marxism is needed here. He appeals to Foucault's stress on surveillance occurring at the "capillary level" of the social organism (1980). Thus, no fundamental social transformation takes place. Rather, by a process of accretion, "powerful electronic systems that measure and monitor transactions for marketing, managing, and controlling groups of people . . . build . . . on processes of surveillance, marketing, and, control bound only by rapidly shrinking technological limits" (1989: 38). He sees in this a subtle process that atomizes individuals, thus eroding the "social community" and violating a "fundamental right of self-determination" (1989: 38).

In several extended discussions of the same issues, Kevin Robins and Frank Webster also start by seeing commercial surveillance as an outgrowth from workplace management, and trace the connections through a consideration of Taylorism. Karl Marx, they observe, expressed the classic insight that capitalist work organization deliberately separates mental from manual labour in order to increase productivity and ensure control. Brainwork, in the scientific management schemes of Frederick Taylor, is concentrated in the "planning department". But if human skills can be expressed in machinery, then the process of subordinating labour may be streamlined further; the culmination of this is Henry Ford's assembly line.

Robins and Webster take this much further, observing that the capitalist-generated gathering of knowledge, skill, and information now takes place well beyond the Fordist factory. In short, "Social Taylorism" appears in the consumer society. The connection

between workplace and household surveillance, they argue, may be found in the marketing practices of General Motors' Alfred Sloan. Back in the 1920s, Sloan pioneered the use of scientific management principles in commodity markets and consumer behaviour. He collected data on buying habits in order to build profiles of customers (1989). Market research, involving the collation of demographic and socio-economic data, placed great stress on the information-control component of such "Sloanism". International Business Machines (IBM) was in the 1930s one of the earliest companies to provide data services to corporations wishing to take advantage of such commercial surveillance.

Today, millions of consumers are subject to efforts aimed at directing their buying behaviour and educating them in consumer skills. New relations of power are exercised, insist Robins and Webster, within the emerging computerized Social Taylorist situation. Indeed, state power should also be seen as part of this equation; it displays Social Taylorist aspects that complement consumerism. The same authors discern many centres of power - perhaps better described by Manuel Castells as "power flows" (1989) or by Lash and Urry as an aspect of "disorganized capitalism" (1987) - within the commercial context. The ghost of Foucault lurks not far behind this account.

Nonetheless, Robins and Webster are not exchanging Foucault for Marx. They add that "in each of the [the power relations] social knowledge and resources are appropriated and transformed into power and capital" (1989: 70). The link with Taylorism does indeed suggest a fairly direct and coercive connection between "capital" and "consumer," and this raises some difficulties. Chiefly, just what kind of power is present here? My own view is that while commercial surveillance undoubtedly links the

power of capital with consumer control, it does so in only indirect and uncoercive ways. That is, coercive means of maintaining social order within capitalist nation-states have shrunk to the point that they are only of marginal importance. The margin is necessary, however, because it leaves in place a group of people, an underclass, if you will, whose non-consuming fate is worth avoiding at all costs. For the majority, though, consumption has become the all-absorbing, morally-guiding, and socially-integrating feature of contemporary life in the affluent societies. Social order - and thus a soft form of social control - is maintained through stimulating and chanelling consumption, which is where consumer surveillance comes in. But this is achieved in the name of individuality, wideness of choice, and consumer freedom.

In what follows, I argue that careful appraisal must be made of the diverse contexts within which commercial surveillance occurs. Moreover, I suggest that it is by no means clear what kind of power relations are displayed in the sphere of consumption. For example, how far is consumption enabled, and how far constrained, by new modes of surveillance? In short, analyses derived from both Marx and Foucault require careful attention. Two specific tasks, appropriate to such attention, are to examine: (a) the "new frontier" of the household as a site of surveillance and; (b) the course of technological innovation in consumer surveillance. By looking at both of these in turn, and then considering their contribution to surveillance capacity, it is possible to obtain a better picture of the contemporary power of consumer surveillance and its role in relation to proposed legislation.

(a) The Domestic Threshold

The precise targeting of households using complex computer power represents a vital tool for marketing in a very lucrative sphere; the commercial data industry is worth fifty billion dollars a year in the United States. The reason for its great success is that the method works for the companies actually selling products and services to the general market. In Britain, for instance, research by Direct Mail Information Services indicates that response to direct mail campaigns remains in proportion to what was sent (Moore). Seven hundred and fifty million pounds worth of direct mail production and postage can generate seven billion pounds of business for companies availing themselves of data entrepreneurial services.

Companies such as Direct Mail Information Services "know where we live" by combining socio-economic with geo-demographic data. In other words, the contents of various apparently unrelated databases are raided to pull together personal information regarding names, addresses, telephone numbers, incomes, and consumer preferences, along with the exact pinpointing and clustering of consumers in different areas but with similar tastes and purchasing powers. This classification includes differentiation by ethnicity and gender. A black lawyer in Dallas, for instance, may be pressed to contribute to Jewish causes because his name is Cohen, and women may receive coupons and sample products just before their periods, or just before and after their babies are born.

A crude behavioural sociology, then, clusters consumers according to their computer-generated "type". Two important things should be noted here, however. The first is that this profiling of consumers uses the micro-analysis of census data prepared by

government agencies. Information that we must yield by law is eagerly devoured by commercial agencies for profit. At this point it is still aggregate data, but nonetheless, given the ease with which information technology facilitates the combination of this with identifiable personal data, new questions do arise. Surveillance using new technology overrides, and thus blurs, conventional distinctions between social spheres once held to be separate. It raises questions about how far governments should permit data gathered for one purpose - which may relate to equity or justice - to be used for quite a different end, namely commercial profit, without the knowledge or consent of the data subjects concerned.

The second note regarding this behavioural consumer sociology is that it depends not only upon technological hardware and software, but upon statistical analysis. Hence it is not merely powerful databases, but also the statistical digesting of facts thus gleaned that produces the desired profile of consumers. Such statistical digesting tells stories about specific demographic groups; that they are from a particular income bracket, tend to have a similar lifestyle and educational experience, or even are from the same ethnic background. Thus, not new technologies alone, but computer power harnessed to statistical techniques, produces these effects.

In addition, telephone numbers are very useful to the new marketers; indeed, the telephone may become more significant than mail as a means of marketing. So-called "smart" telephone networks are now used to identify callers who use tollfree numbers to place orders or to make customer enquiries. The receiver of the call often has immediate access to the caller's purchasing power and preferences with the details appearing on a

screen even as the caller waits to be answered. What is new here is that the screening process occurs instantly and without the caller's knowledge. But, once again, larger scale public policy is involved, in that such "smart" telephone capabilities depend upon the establishment of Integrated Services Digital Networks (ISDNs) that have been extremely deregulated in several countries in recent years.

In Oakbrook, Illinois, for example, Telesphere Communications offers a service to "900" subscribers allowing the company to peg the location of incoming calls using an area code and the number's three digit prefix on an ISDN system. PRIZM, a Virginia database company, supplies the demographic data to Telesphere. PRIZM classifies different neighbourhoods according to characteristics useful to the marketer. Here are the results of their behavioural sociological analyses: "Furs and Station Wagons" are people who are "big spenders with new money". Less desirable to the companies in question are clusters like "Emergent Minorities" who are "almost 80 percent black with the remainder largely composed of Hispanics and other foreign-born minorities . . . below-average levels of education and below-average levels of white employment. The struggle for emergence from poverty is still evident in these neighbourhoods" (Stix, 1991: 152). Without their knowing it, then, customers' residence, income, and background are revealed to salespeople through their telephone number. These salespeople then choose their selling strategy on the basis of that information.

In the above-mentioned examples, the household threshold is crossed by means of the letter-box and the telephone line. Since the 1980s, however, the advent of "home networking" in some countries has brought a novel dimension to electronic surveillance:

two-way interactive systems linking external services directly with the household. Dressed as the potential realization of older versions hitherto only partially fulfilled, home networking - where it exists - represents a further major extension of the practices involved in electronically collecting, storing, processing, and retrieving personal data. In short, home networking means that the act of purchasing or making other financial transactions can now take place beyond conventional stores, banks, and shopping malls.

In North America, home networking has emerged haltingly, and where it has done so, it has rightly attracted the attention of social analysts. In two Canadian studies, for example, David Flaherty (1985) and Kevin Wilson (1988) discuss the implications for surveillance and privacy of two-way interactive services. Flaherty acknowledges consumer benefits of such systems but warns about the "potentially darker - surveillance - side". He emphasizes privacy concerns and how the cable companies running them may be subject to self-regulation with regard to "privacy". Beyond self-regulation, Flaherty argues that individuals should have clear rights to use the courts when third-party access to personal data has been granted without consent.

Wilson, on the other hand, is critical of any "balance-sheet" approach to the society/technology relationship, and is instead concerned that interactive systems are subject to "economic pressures designed to transform human activities into marketable commodities" (1988: 9). While not unconcerned about the "privacy" aspects of home networking, he also invokes the notion of social management to analyse its further potential effects. Wilson suggests that the use of anonymous data, gleaned from two-way services by market researchers and forecasters, also carries dangers of social control. As

he says, "surveillance in itself does not ensure compliance, but an awareness of its presence clearly does so by subtly encouraging the individual to internalize the rules" (1988: 97).

In Wilson's view, social responses to corporate initiatives are engineered by creating and manipulating needs that have never been subject to public debate. Social management, for Wilson, thus threatens democratic polity by exacerbating inequities of knowledge, and making consumers more and more vulnerable to corporate power. If we add to this an issue raised above, that consumer surveillance makes extensive use of official data, it becomes clear that ethical and political questions of some magnitude attend this crossing of the domestic threshold.

(b) New Technologies for Surveillance

The example of commercial surveillance by two-way cable raises the important question of how far we should examine emerging, as opposed to already existing, surveillance practices. Perhaps comments should be held back until the real impacts of such new technologies are known. After all, technological potential is never social destiny. New artefacts and technological processes are shaped in different ways by varying social, political, and cultural processes, and unanticipated factors enter into their economic or technical success. Two-way services based on cable television simply are not at the forefront of surveillance concerns in the late 1990s.

The major problem with this approach, however, is that once new systems are firmly established, they become very difficult to alter, if that strategy seems to be called for. Moreover, their use may generate related technological innovations which quickly

multiply the social consequences, as in the case of Automated Bank Machines (ABMs). Also, the pace of technological advance is often very rapid, and the argument is frequently made that social safeguards should be built into new technologies.

ABMs, to take up the example, rapidly have become a feature of late twentieth-century life. The banks which use them clearly benefit; the costs entailed are less than half of those for a human teller. The chief consumer benefit is probably convenience; ABMs permit the 24-hour customer, seeking one-stop financial services. But once again, from a surveillance perspective, ABMs enable banks to pinpoint personal preferences and even physical movements and to add these to the profile built from transaction patterns. Now cardholders can obtain services from banks other than their own, especially where one bank-holding company such as Citicorp own many smaller ABM nets.

Another example of a new surveillance technology that promises to contribute to the ever-growing traffic in personal data is smart cards. Smart cards have embedded within them tiny chips of integrated circuitry, enabling the storage of data in the card. Numerous uses have already been found for these, especially in Europe, where phonecards are commonplace; in addition, they have been used by banks and health services as well by private companies for internal security purposes.

In Canada and the United States, various smart card experiments have also been tried or are underway, on both large and small scales. A Vancouver restaurant owner, for instance, uses a smart card that is not traceable back to the individual cardholder. On a much larger scale, are pilot schemes that store detailed data in relation to a number of different agencies. The Quebec government, for example, is currently considering

proposals for the development of a multi-purpose smart card. The card under consideration would be used for all program delivery, including such things as hunting and fishing licences. A similar proposal in British Columbia using laser photo smart cards would merge drivers' licences, welfare cards, and health cards. In his annual report, the federal Privacy Commissioner of Canada argued that smart cards are quickly becoming a "plastic panacea" as bureaucrats and private sector administrators attempt to deliver programs more efficiently (OPC, 1996: 6).

It is thus critical - as well as entirely appropriate - for novel uses of information technology to be monitored by social analysts. New services, based on extensions of existing technology, appear constantly. Consumer capitalism continually innovates in the quest for new markets and maintained profit shares. Furthermore, the examples chosen here suggest that the tendency is for the asymmetrical relationship between corporate organization and individual consumer to be exaggerated by every new gadget and service. Claims regarding consumer benefit - some of which may be perfectly legitimate - hardly have time to be tested before the next innovation appears. And issues of social division, reflected accurately in the consumer surveillance described in this section, and human dignity are seldom even considered. As such, it is imperative that such trends be subjected to responsible social analysis, even if they continue to lag behind the perpetual renewal of technology.

Consumer surveillance in the late twentieth century entails a massive intensification of surveillance throughout society, and technological innovation is constantly enhancing its capacity. Subject transparency is especially augmented. Connections with the nation-state

and with the capitalist workplace - Social Taylorism - should be pursued, but consumer surveillance must also be viewed as part of an emerging set of social arrangements, articulated with consumption, that is also a departure from what we already know about surveillance. Here comments made about rapidly changing technologies must be borne in mind; the need for fresh thinking and flexible policy-making is paramount. The Canadian government recognizes this insofar as it acknowledges that "modern information technology has made it infinitely more feasible for businesses and other private institutions to amass and exchange data . . . advances in computer and network technology have multiplied and magnified the challenges to privacy".[3] The connections between these challenges and a theory of the social order of consumption, however, have yet to be made.

Indeed, the systematic monitoring and intervention in personal tastes, fashions, and symbols by means of the kinds of processes indicated in this section call for a general recalibration of social theories of surveillance. In this regard, while Zygmunt Bauman's work on consumerism as a central feature of postmodernity is singularly important, even he has little to say about how sophisticated surveillance of consumers is articulated with it. Nonetheless, in our quest for a critical perspective, his comments on the duplicity of consumerism are worth heeding. One face of this is the (false) promise of universal happiness following from freedom of choice, while the other is that the problem of freedom (supposedly) is resolved once consumer freedom is offered (1992). These hidden

---

[3] Speech by Allan Rock to the *Eighteenth International Conference on Privacy and Data Protection*, Ottawa, Ontario, September 18, 1996.

assumptions on which the social order of consumerism operates cannot be ignored within any responsible theory of consumer surveillance.

Surveillance theory must take into account, therefore, both how data-subjects are constituted as consumers and how their patterns of consumption are channelled through commercial surveillance. With regard to the former, vital questions of human identity and dignity are raised, alongside issues of freedom. And touching the latter, questions of social division, both between consumers and non-consumers and along the fault lines of gender and ethnicity, provoke critical analysis in terms of justice and social participation.

Though we cannot predict the long-term consequences of structuring social participation around consumption, or of limiting personal or collective responsibility by means of the disciplines of consumer surveillance, it seems clear that they add up to some social circumstances not entirely precedented in previous modern experience. However much consumer surveillance practices may resonate with Taylorist methods, it must be recognized that the leading principle of the consumer order is pleasure, not pain or coercion. What remains to be socially analysed and politically challenged is the peculiar threat of consumer surveillance to exacerbate social division and undermine human dignity.

Situating Surveillance: Surveillance, Modernity, and Beyond

The modern state is best thought of as an advanced form of organization whose administrative bureaucracies are concerned above all with surveillance and maintaining social order on the one hand, and economic management on the other. These tasks

embrace a wide spectrum from registering births, marriages, and deaths, through collecting and redistributing taxes, to maintaining armed forces to defend territory and interests. Nation-states thus play a major role in manipulating the settings in which human activities occur and controlling their timing and spacing.

However, we have seen historically that this was not always the case. For example, the Israelite Census, mentioned at the beginning of the chapter, was originally a means of regrouping after the flight from slavery in Egypt and of ensuring some semblance of military order among people who had shortly before been a ruthlessly exploited minority underclass. It was only later that the census came to serve as a way of apportioning land as wanderers settled in Palestine. Why did the Israelite Census acquire new designs and functions? What happened between the Israelite Census of the fifteenth century BC and the interlocking networks of government and administrative databanks of the twentieth? Why do we inhabit such extensively administered societies today? The brief answer, explored in detail in this chapter, lies in the birth of modern society, with its constitutive components of the nation-state and industrial capitalism.

Stated simply, this chapter has argued that modernity established surveillance as a central social institution. The rudimentary practices of traditional and feudal societies were vastly intensified and made more systematic in the modern era. And the surveillance capacities of organizations were constantly enhanced, while the routines of everyday life became transparent as never before. Certain conclusions may be drawn from this which may yield clues for the further analysis of surveillance today.

First, there is the question of power. We have seen how surveillance progressively replaces physical coercion as a means of maintaining order and co-ordinating the activities of large populations in the contexts of capitalism and the nation-state. Surveillance also connects closely with knowledge, expressed variously in the specialized tasks of the bureaucratic official or the business manager, both of whom are increasingly separated from those whom they oversee. Being "in the know" clearly has consequences for discipline and power.

However, these consequences must be analysed in relation to the fact that modernity includes several overlapping dimensions. For example, the bureaucratic organization is found in settings as diverse as the capitalist enterprise, the army, and the government department. Similarly, Marshall's account of the widening of citizenship rights takes us through different social spheres, each of which carries with it implications for the monitoring and documenting of individuals. Thus, modernity may not be reduced to any one of its dimensions. By the same token, we should also beware of seeing surveillance power as exclusively related to any one aspect.

Second, there is the experience of surveillance. Part of the answer to the question of power is that surveillance power is patently not absolute. Surveillance originates in a paradoxical fashion - being the outcome of the quest for citizenship, and also of greater centralized state control - and is experienced with ambivalence. For example, we are both grateful for the services or convenience that contemporary surveillance systems afford, and irritated or offended when, say, inaccurate records are used to make decisions about our opportunities and life-chances. Perhaps Foucault is right to say that power is a

strategy; certainly scope exists for "answering back" in at least some surveillance situations. Surveillance seems to enable as well as constrain.

Third, and finally, there is the political question. Does control of information become the key issue in contemporary "surveillance societies"? We have seen how surveillance capacity has grown systematically in modern societies. James Rule suggests that this has to do with four things: the size of files, their degree of centralization, the speed of information flow, and the number of contacts between administrative systems and subject populations (1973). If we contrast the personal and indirect control involved in, say, the Israelite Census of the fifteenth century BC with the direct control that we have with multiple organizations today, we can begin to appreciate how surveillance capacities have grown. It is not difficult to see why questions of information control are highly significant and are increasingly politically important.

This is reflected, for example, in Industry Canada's announcement that "The first challenge facing Canadians is to facilitate Canada's transition into the knowledge society" (1996: 3). Similarly, Allan Rock, the former Minister of Justice, suggests that "Canada has been evolving rapidly from a resource-based economy to one based on information and knowledge . . . in this environment, more and more private institutions are collecting, using, and exchanging information about our consumption habits and services".[3] This explains the decision to "bring forward proposals for a legislative framework governing the protection of personal data in the private sector" (Industry Canada, 1996: 25). Thus,

---

[3] Speech by Allan Rock to the *Eighteenth International Conference on Privacy and Data Protection*, Ottawa, Ontario, September 18, 1996.

legislation, an anti-surveillance measure, is an "idea whose time has come" insofar as surveillance has developed as a part of everyday life with the historical rise of modernity.

Chapter Three: Situating Surveillance Theoretically and Critically

Understanding Surveillance: From Big Brother to the Electronic Panopticon

We have seen in Chapter Two how, in the twentieth century, the medium of surveillance shifted decisively from paper files and direct observation to computer files that filter data through a grid of electronic language. In addition, we have seen that the sites of surveillance were enlarged to include the new and vast terrain of consumerism, which simultaneously may be viewed as a source of social order in itself. Theories attempting to explain contemporary surveillance must be aware of these trends. This can be accomplished only by locating surveillance in its broader structural and historical context. In this way, it is possible to distinguish between the short-term aberration from some norm and the long term break with existing conditions, between the socially significant and the trivial or the transient. Chapter Two placed electronic surveillance in just such a context. By showing where surveillance came from, what is new about it, and what are its future prospects and wider implications, the chapter demonstrated that electronic technologies have been introduced in order to augment and sustain surveillance activities on an even larger scale than that known in the era of the Victorian clerk.

By exploring the ways that surveillance technologies are used historically - that is, how they help to augment, supersede or diminish the importance of already existing practices - it is also possible to place current debates over computer power and social control in the context of other angles: social theory, the politics of policy making, and social movements. It is to the first angle that the dissertation now turns. In this chapter, I suggest that the concepts of Big Brother and an electronic Panopticon have made frequent appearances within analyses of electronic surveillance. This chapter traces briefly the

history of these concepts, with particular emphasis on the Panopticon. It argues that while these images have considerable illuminative power, their ability to serve as "total" explanatory tools is limited. This is because both models are dystopic, concerning - in critical treatments - fearful futures where surveillance equals control, constraint, the probing eye, and an absence of freedom. As such, I suggest that the prominent models of Big Brother and the Panopticon fail to theorize the two faces of surveillance explored in the last chapter. Surveillance, as I have argued, spells both control *and* care, proscription *and* protection; it is paradoxical and ambiguous, exhibiting more than one face.

The inability of Big Brother and the Panopticon to explain the two faces of surveillance translates into a misleading, one-dimensional understanding of surveillance and, worse, an inability to resist the insidious sway of paranoia and pessimism which obviously grips these models. As an alternative, I propose that the social analysis of surveillance be harnessed to a consideration of elements of the "good society" as opposed to those of the "bad" as seen in the dystopian models deriving from Orwell and Foucault. To this end, I draw on the practices of openness, accountability, and co-operation derived from Geoffrey Brown (1990) in order to sketch a vision of the future that catches some elements of hope. The chapter concludes by arguing that imaginative social analysis, informed by constructively critical theory based on the above practices, would not only go a long way towards relieving us of the paranoia and fatalism bequeathed to us by the dominant models, but would also create space for alternative models of understanding and action.

Orwell's Dystopia

When I tell people that I am studying surveillance, and in particular investigating the ways that our personal details are stored in computer databases, the most common reaction is to invoke George Orwell; "This must be the study of Big Brother". A perfectly understandable response given that *Nineteen Eighty-Four* is often taken to be about the power of technology and social control and about the loss of privacy resulting from living in such a transparent society. For example, in *Nineteen Eighty-Four*, Winston Smith, who attempts to think for himself, is eventually crushed into conformity by the surveillance state which depends on a huge bureaucratic apparatus, "thought police", and the figure of "Big Brother" to maintain constant vigilance over the intimate lives and relationships of each citizen. Thus, total control in Orwell's Oceania is made possible by centralization. Today, governmental and commercial "centres" retain access to computerized files on major populations, so it is not surprising that *Nineteen Eighty-Four* has been readily translatable into the language of microelectronics and information technology, with their supposed threats.

Orwell was astoundingly prescient, which is of course the reason why his work has not only survived but maintained its interest. In short, Orwell observed the growing centrality of information in the operations of the nation-state. In Oceania, there was even a "Ministry of Truth" to deal with such matters as the creation and destruction of information. Today, computer technology facilitates the construction of new categories of data, a process that is encouraged by the penchant for statistical analysis within organizations. Moreover, the same technologies make possible the electronic erasure of

data, either without the trace, or traceable only by experts. Both processes are significant to the "surveillance society".

For one thing, the malleability of data may render the Weberian confidence in the reliability of the record somewhat naive. The electronic trail may be eradicated without a trace, which leads to larger questions of how far data may be trusted. For another, sauce for the goose is sauce for the gander, and the malleability of data may also be seen in the phenomenon of fraudulent IDs. With the twentieth century rise of credentialism and the constant demand for identification, the temptation to invent or enhance personal documentary details has for some been too difficult to resist. Obtaining goods, services, benefits or employment may all be facilitated by a variety of ways of distorting identity or biographical details. Technology is not simply a tool of dominant social groups.

The focus on novel techniques for handling information also rings true in the context of computing and administration. As I have shown in the previous chapter, it is information *technology* that is especially significant for surveillance. The national databank, for instance, is exactly what one would expect to find in an Orwellian surveillance society. Recognizing this, American officials denied during the 1970s that such a databank would be created. Yet all employees of the United States federal government are now listed in a single database that is used for matching purposes.

Another significant feature of Orwell's "Big Brother" surveillance is that it was imperceptible. Those under surveillance were unsure whether there was any time they could relax. Like the Panopticon - and in other literary treatments of the surveillance theme, such as Franz Kafka's *The Castle* and Margaret Atwood's *The Handmaid's Tale* -

this model of undetected surveillance keeps those watched subordinate by means of uncertainty. One simply complies because one never knows when "they" might be watching. Information technology enables surveillance to be carried out in ways even less visible than those available in Orwell's, let alone Kafka's, day.[3]

Finally, two further points, to do with dignity and division, may be made that underscore Orwell's relevance for contemporary surveillance. *Nineteen Eighty-Four* has been used to connect transparency of behaviour with the theme of privacy. Yet there is a sense in which Orwell's focus was less narrow than that. For him, privacy was an aspect of human dignity. Winston Smith, for instance, finally caves in, betraying his girlfriend Julia and declaring his love for Big Brother, *not* when his privacy is invaded but when deprived of his dignity in a confrontation with rats. From that moment, Winston's dignity is merged with Big Brother's. His very personhood is impugned. The challenge of electronic surveillance is missed if it is reduced to a concern merely with privacy.

As for division, Orwell clearly shows how power is maintained at a broader level through the diverse character of surveillance. In his *Visions of Social Control*, Stanley Cohen stresses this fact of Orwell's work (1985). The middle class and Party members needed careful thought-control and surveillance. Inclusionary controls reign here. But the proles, who formed 85% of the population, could safely be left in their ghettoes, "working, breeding, and dying" (Orwell, 1954: 60). Their lot is exclusion. The important

---

[3] Gary Marx makes much of this connection between computer surveillance and detectability. See "The Iron Fist in the Velvet Glove: Totalitarian Potentials within Democratic Structures," in J.F. Short (ed)., *The Social Fabric*, Beverly Hills, CA: Sage Publications, 1986 and *Undercover: Police Surveillance in America*, Berkeley: University of California Press, 1988.

point here is the role of surveillance in different modes of social control, rather than the details of Orwell's analysis.

Things have changed since Orwell's time, and consumption, for the masses, has emerged as the new inclusionary reality. Consuming is paraded as a matter of personal choice. Freedom to select between alternatives is touted as the acme of the unconstrained life. Only when the customer runs into debt or when inaccurate records are used, does the weight of much more coercive action descend. Those who do not deviate from desirable levels of consumption regard most forms of commercial surveillance as aspects of convenience and comfort in the consumer society. Temporary scares over privacy may surface from time to time, but these are mere blips in a smoothly running megamachine that constantly gathers, stores, matches, processes, and sells personal data.

Anyone wishing to grasp the nature of contemporary surveillance must reckon with this reality. Whereas the major threat, for Orwell, came from the state, today consumer surveillance poses a series of novel questions which have yet to find adequate analytical and political answers. A perfectly plausible view is that in contemporary conditions, consumerism acts in its own right as a significant means of maintaining social order, leaving older forms of surveillance and control to cope with the non-consuming residue.

Having said that, however, some further qualification is in order. While consumerism may correctly be viewed as a means of social control, it differs from other types of such control. Those targeted for direct mail and other forms of personalized advertising are objects of an attempted channelling of behaviour. Companies wish to

include rather than *exclude* them. The important distinction between exclusionary and perhaps punitive forms of control, which may be coercive, and more subtle ones, which rely on creating desired behavioural conduits, should be borne in mind as the dissertation proceeds.

This in turn also ties in with a more general theme in the history of social control; the progressive uncoupling of violent and non-violent methods of social control. Orwell tended to retain the links. Both jackboots and Big Brother have their place in Oceania. This is not surprising given that Orwell's own experiences were of the Spanish Civil War, Stalin's Soviet Union, and Mussolini's Italy. Many have imagined that Orwell had only these obviously totalitarian regimes in mind in writing *Nineteen Eighty-Four*. However, it is more than likely that he intended its application to be broader. As a democratic and libertarian socialist, Orwell was quite aware of certain authoritarian tendencies within capitalist societies. What he may not have foreseen was that new technologies might eventually permit surveillance tending towards totalitarianism *with democratic processes still neatly in place*. As Gary Marx observes, the velvet glove may hide the iron fist (1986).

Social analysis of surveillance that begins with Big Brother produces some useful insights. The fact that electronic technologies have been augmented considerably since Orwell's day does mean that his account needs some updating, but it does not render it irrelevant. Much of what Orwell wrote still stands, and deserves attention, but the specific ways in which we must go beyond Orwell also need to be explored. At this point, then, I

turn to the Panopticon and examine whether as a model it can compensate for the shortcomings of Orwell's dystopia.

The Panopticon from Bentham to Foucault

Every now and then a concept catches the critical imagination because it seems to capture neatly some feature of contemporary society. "Anomie", "network", "labelling", "mass society", and many others qualify as examples. The Panopticon holds promise as just such a concept. Originating as Jeremy Bentham's eighteenth century architectural plan for a prison, the Panopticon became the centrepiece of Michel Foucault's theory of surveillance. Although Foucault made no allusion to computers, the Panopticon now makes frequent appearances in discussions of electronic surveillance.

Foucault illuminates the connections between the Panopticon and modernity by showing that it forms the watershed between punitive and reforming disciplinary practices. Enlightenment reason, concerned with empirical observation and classification, and related to the rational reproducing of social order, is neatly expressed here. The theme of exploiting uncertainty as a means of controlling subordinates appears in the Panopticon as well, having obvious resonance with the unobtrusive monitoring of which new electronic technologies are capable. However, this in turn propels us into the debate over postmodernity. A hallmark of modern thought is the way that individuals are placed centre-stage in history. But postmodern discourse pushes such actors into the wings, and this seems to echo what happens with electronic surveillance. If the supposedly

"personal" details of intimate, everyday life circulate beyond our control within remote databases, where now is the human "centered" self?

Bentham, a British philosopher and social reformer, published his plan for the Panopticon penitentiary in 1791. Essentially, it was for a building on a semi-circular pattern with an "inspection lodge" at the centre and cells around the perimeter. Prisoners, who in the original plan would be in individual cells, were open to the gaze of the guards, or "inspectors," but the same was not true of the view the other way. By a carefully contrived system of lighting and the use of wooden blinds, officials would be invisible to the inmates. Control was to be maintained by the constant sense that prisoners were watched by unseen eyes. There was nowhere to hide, nowhere to be private. Not knowing whether or not they were being watched, but obliged to assume that they were, obedience was the prisoner's only rational option. Hence Bentham's Greek-based neologism; the Panopticon, or "all-seeing place" (Bentham, 1843).

The Panopticon was to be a model prison, a new departure, a watershed in the control of deviance and a novel means of social discipline. Bentham invested more time and energy in this than any other project - and "mourned its failure more passionately" (Himmelfarb, 1968: 32). He saw in it "a great and new invented instrument of government" and believed the panoptic principle held promise of "the only effective instrument of reformative management" (Bentham, 1843: 39). In a closing eulogy, that he later repeated in the preface, he made the famous claim, "Morals reformed - health preserved - industry invigorated - instruction diffused - public burdens lightened -

Economy seated, as it were, upon a rock - the Gordian knot of the Poor Laws not cut, but untied - all by a simple idea in Architecture!" (1843: 39).

Bentham's apparently utopian enthusiasm for the Panopticon had personal, political, and cultural origins. Personally, he hoped to reap financial benefit from an entrepreneurial stake in the project, and to raise his status profile from being its first director. Politically, the Panopticon promised a local, non-religious reform over and against the Evangelical and transportation-to-Australia alternatives that were currently on offer at the time. And culturally, the Panopticon epitomized the kind of "social physics" so popular with *philosophes* of his day. It neatly translated La Mettrie's *L 'Homme Machine* into an architectural reality.

Ironically, while it appears that no prison was ever built exactly along the lines Bentham had in mind, and he certainly failed to persuade the British government to invest in it, the principles embodied in the Panopticon were to have a widespread influence. For example, the key principle was inspection, though inspection of a specific kind. Bentham's Panopticon represented a secular parody of divine omniscience and the observer was also, like God, invisible. Thus, "the more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment be attained" (Bentham, 1843: 40). And if such constant supervision proves impossible, prisoners should be given the *impression* that the gaze is unwavering.

Bentham's innovation, then, was not just to inspect, or even to ensure that the gaze is asymmetrical, but to use uncertainty as a means of subordination. The

asymmetrical gaze created uncertainty which in turn produced surrender. Asymmetrical surveillance joined the whole modern project of destroying the certainties of alternative powers, wherever they still lurked (Bauman, 1991). This is why the Panopticon *principles* were so significant.

The inspection principle suited purposes other than prisons, according to Bentham. Indeed, Bentham got the original idea of the Panopticon from his brother's workshop in Russia. And he advertised the virtues of the Panopticon as being appropriate for any context in which supervision was required; for " . . . punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curing the sick, instructing the willing in any branch of industry, or training the rising race in the path of education" (1843: 40). Foucault argues that panoptic control has diffused through many of these spheres.

Two other principles attached to the Panopticon in the specific context of the penitentiary. One was the "solitude" or isolation of the inmates, the other was to allow the prison to be run as a private enterprise by outside contractors. Solitude would extend even to having private toilets for prisoners, and to holding chapel services from a central position above the inspection lodge, without prisoners moving from their cells. Inmates were to be atomized, secluded. As for running the prison by contract, this would enable profit to be made and prison governors to be held in unaccustomed esteem.

Bentham readily defended his Panopticon from any misplaced liberal attack. Might it be though "despotic", or might the result of "this high-wrought contrivance . . . be constructing a set of *machines* under the similitude of *men?*" (Bentham, 1843: 64). Let

people think so if they wish. Such criticisms miss the point, namely, "would happiness be most likely to be increased or decreased by this discipline?" (Bentham, 1843: 64). Here is control, and clean control at that. Much better, Bentham commented, than something like Addison's bizarre sounding proposal to "try virginity with lions" (Bentham, 1843: 64). There one saw blood and uncertainty; "here one sees certainty without blood" (Bentham, 1843: 64). Of course uncertainty still exists for those subjected to the Panoptic regime. Indeed, the "machine" depends on it. Certainty resides in the system, and, one might add, with the inspector, the one "in the know".

This kind of certainty, sought by Bentham in the Panopticon, epitomizes for Foucault the social disciplines of modernity. Whereas in earlier times the failure of social control would result in punishment that was public and brutal, modernity introduced clean and rational forms of social control and punishment. The unruly crowd is rendered manageable; no plots of escape from prison, no danger of contagion if they are patients, no mutual violence if they are mad, no chatter if schoolchildren, and no disorder or coalitions if workers. The crowd is replaced by a "collection of separated individualities" (Foucault, 1977: 201). As Foucault says, Bentham made "visibility a trap".

In the following important quotation, Foucault summarizes his understanding of the major effect of the Panopticon (1977: 201):

> to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they themselves are the bearers.

In the Panopticon, discipline crossed what Foucault calls a "disciplinary threshold" in which the "formation of knowledge and the increase of power regularly reinforce each other in a circular process" (1979: 204). Older, more costly and violent forms of power fell into disuse and were superseded by "a subtle, calculated technology of subjection" (Foucault, 1977: 221).

Social theory is indebted to Foucault for his theory of surveillancee, touching as it does on both aspects of its power; the accumulation of information and the direct supervision of subordinates. The former is found in the detailed files held on each Panopticon inmate, the latter in the architectural potential of the building itself. Acknowledging Foucault's contribution, Giddens observes that in modern times "disciplinary power" is characterized by "new modes of regularizing activities in time-space" (1985: 183). Observation is central to these modes, and thus the Panopticon epitomizes such disciplinary power.

However, Foucault also insists that such power is typically present throughout the institutions of modernity, in all kinds of administrative contexts. "Is it surprising," asks Foucault rhetorically, "that the cellular prison, with its regular chronologies, forced labour, its authorities of surveillance and registration, its experts in normality . . . should have become the modern instrument of penality?" (1977: 228). But not only that; he goes on, "Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?" (1977: 228). What for Bentham was an aspiration is for Foucault a social reality - the panoptic principle diffusing through different institutions. This

assumption, often questioned within the context of administrative power, must be re-addressed in the context of electronic surveillance.[4]

The perverse irony is that Foucault himself seems to have made no comments about the relevance of panoptic discipline to the ways that administrative power has been enlarged and enhanced by computers, especially since the 1960s. Yet surely we see nothing less than the near-perfection of the principle of discipline by invisible inspection *via* information gathering. Or do we? Today, no shortage exists of social analysts prepared to complete Foucault by making the connections explicit. Thus, I turn next to explore the extent of that link; can electronic surveillance be thought of as panoptic power? In other words, does panoptic power match the empirical realities of social order in today's contemporary advanced societies?

Is Electronic Surveillance Panoptic Power?

In order to obtain some analytical purchase on the question of electronic panopticism, this section makes use of Giddens' distinction between two major axes of surveillance. He proposes that social theory consider two levels: first, surveillance is the accumulation of coded information, seen in what he calls the "internal pacification" of nation-states. This is bound up with the growth of bureaucratic administration, defence, and policing. Second, surveillance refers to the direct monitoring of subordinates within

---

[4] The Panopticon may also be seen in relation to other kinds of technique, particularly that using biotechnology. But the surveillance power of biotechnology depends, nonetheless, upon (micro)electronics.

the capitalistic workplace that has become the key to management in the twentieth century (1985).

Giddens admits that the two senses of surveillance belong quite closely together. Indeed, only when thought of together can the twin processes of surveillance illuminate the historical association of the capitalistic labour contract with the state monopoly of violence. Still, he maintains that they should be analytically distinct. I begin by following this distinction, and respecting it, looking first at the treatment of criminality and deviance as a central aspect of "state" surveillance. Next, I examine the putative Panopticon of capitalism, starting with the workplace. However, this may oblige us to rethink the Giddens distinction, for two reasons: one, capitalism in the late twentieth century focuses at least as much "management" attention on the marketplace as the workplace. And two, the application of information technologies may be encouraging a convergence between different surveillance activities.

The persistence of panoptic principles in contemporary society has been noted by those studying general trends in social control, such as Stanley Cohen, and by others examining specific practices involving new technology in policing. Cohen, for instance, investigates the later twentieth century shift towards crime control "in the community" that includes rather than excludes offenders. He notes the ways that panoptic ideas are present in methods of "technological incapacitation" (1985: 222). Radio telemetry, or electronic tagging, allow relatively minor offenders to live "freely" at home, or even to go to work while wearing a computerized device on the ankle. This tag involuntarily obliges the offender to remain in touch with some central control. Cohen relates this to the

Panopticon in that the wearer is constantly supervised and participates in the process, but cannot verify it.

Gary Marx's analysis of American undercover police work takes this much further, noting numerous ways in which electronic technologies portend the "new surveillance". Particularly relevant here are these characteristics, as described in Chapter Two: they are invisible (or of low visibility), involuntary, capital rather than labour intensive, involve decentralized self-policing, introduce suspicion of whole categories of persons rather than targeting specific individuals, and are both more intensive and more extensive. He sees the state's traditional monopoly over the means of violence as giving way to new controls: manipulation not coercion, computer chips not prison bars, remote and invisible tethers, not handcuffs or straitjackets. Marx cautions that these panoptic shifts may be "diffusing into the society at large" (1988: 207).

In another American study, Diana Gordon subjects the National Crime Information Center (NCIC) to analysis as a panoptic "machinery of power" (1986). Her central concern is simply expressed; "With the national computerized system, the entire function of crime-control, not just the prison, becomes a 'panoptic schema', with the record a surrogate for the inmate and all of law enforcement as warden" (1986: 487). Gordon is at pains to argue that the presence of panoptic tendencies spells dangers often unperceived by those working closest to the NCIC. Certain structural social changes may be occurring, she suggests, and therefore it is mistaken to see the issue as merely one of infringing civil liberties. For instance, in many states at least a third of criminal record requests are for non-criminal purposes, mainly employment and driving licences. Like

Gary Marx, Gordon believes that the effects are societal; "and then we are all enclosed in an electronic Panopticon" (1986: 487).

The distinctions between criminal record databases and more general computerized systems for government administration have become increasingly blurred over the past few decades, especially as computer matching has become a more widespread practice. This refers to the linking of records from different databases to track offenders or to limit abuse, such as tax evasion or welfare fraud. Employment records may be checked, for example, to prevent welfare claims being made by people receiving salaries (Reichman, 1987).

Oscar Gandy, who makes extensive use of the Panopticon model in his work on modern surveillance systems, suggests other ways that new technologies extend their reach within a government context. For example, in addition to the massive databases of the Department of Defence and the Central Intelligence Agency, the United States Internal Revenue Service is a major collector of personal data, used to identify non-reporters and under-reporters. Political parties also seek to strengthen their position by using computerized surveillance methods to affect public opinion (Meadow, 1985; Weiss, 1988).

Turning now to the second area, we find that the Panopticon has also been rediscovered in capitalism. In the preceding chapter, we saw that the debate over whether or not the adoption of new technologies represents intensified workplace control within capitalism is complex and inconclusive. Shoshana Zuboff's ethnography, *In the Age of the Smart Machine*, for instance, takes the view that computers in the workplace have a

tremendous transformative capacity. Parallelling authority as the "spiritual basis of power," she examines technique as the "material basis of power" (1988). The key to contemporary management technique, she argues, is panopticism, enabled by the use of new technologies.

The extremely precise computer systems of today's organizations permit minute monitoring of events and performances within the workplace. At one of the workplaces investigated by Zuboff, a highly automated pulp mill, a small explosion occurred in the early hours of the morning. By scrutinizing the "Overview System", a bird's-eye view of the whole operation which was constantly recorded at five-second intervals, management could determine the exact cause of the accident - for example, equipment failure, poor decision-making, or a sleepy operator? (1988: 315-17). Workers at such sites are thus highly transparent to management even in the apparently small details of day-to-day routine. This heightened visibility - also noted by researchers looking at computerization in much smaller contexts such as ordering in restaurants and taxi-calling systems (Rule and Attewell, 1989) - Zuboff connects with the Panopticon.

Other aspects of panoptic power are clearly visible in Zuboff's account of the computerized workplace. In particular, she discusses the allure of panopticism for management, which - neatly echoing Bentham - is "the promise of certain knowledge". For example, increased reliance upon the "facts" produced by the computer systems generates new management styles in her account. Employee performance appears as "objective" data, which often correlates with another panoptic feature, the certainty of

punishment. Apparently, the firing process tends to be shortened from around one year from the start of the dispute to something much more immediate. (1988).

Operators within the ubiquitous digital "gaze" of such computer systems, and without the more familiar face-to-face relationships with superiors, may seek modes of resistance, but compliance appears more common. Information systems "can transmit the presence of the omniscient observer and so induce compliance without the messy conflict-prone exertions of reciprocal relations (Zuboff, 1988: 323). Zuboff comments that in workplaces where workers as well as management had access to the personal data collected on the systems, "anticipatory conformity" was exhibited, showing that the standards of management had been internalized by workers. This gain seems to be a case of Foucault's "normalizing discipline" of the Panopticon.

Interestingly enough, though, Zuboff does not try to generalize her findings to a societal level. She sees no need to; for her, the transformations within the workplace are striking enough. Her modesty may be wise. Others, however, have argued that some of the kinds of management strategies made possible by the new use of information technology are now being applied in the marketplace as well as in the workplace. In this way, it is suggested, the panoptic power of surveillance spills over into society at large, but now the vehicle is commercial organization, not government administration.

This link is made directly by Frank Webster and Kevin Robins, for instance, who argue that information technologies facilitate the massive extension of Taylorist principles of scientific management from the realm of production into the realm of consumption. As they say, "teleshopping", global and targeted advertising, and electronic market research

surveillance all combine to establish a more "efficient network marketplace" (1989). In this case, surveillance is accomplished by means of gathering transactional information such as itemized telephone bills, credit card exchanges, and bank withdrawals. The whole process of using transactional information to try to influence consumer behaviour is sometimes called "social management" (Mosco, 1989). Oscar Gandy takes up the same themes, focusing particularly on the ways that personal consumer data has become a vital "information commodity" within contemporary capitalism (1993).

This picture is very similar to one painted, in richer Foucauldian terms, by Mark Poster. For him, the world of consumer surveillance amounts to a "Superpanopticon" because the panopticon now has no technical limitations (1989). The Panopticon was invented for a new industrial capitalist society. Today "the population participates in its own self-constitution as subjects in the normalizing gaze of the Superpanopticon" (Poster, 1990: 97). Poster's analysis occurs in the context of a study of the "mode of information" which, he explains, "designates social relations mediated by electronic communications systems which constitute new patterns of language" (1989: 123).

The technology of power in Poster's Superpanopticon does two things. First, it imposes a norm, disciplining its subjects to participate, say, by filling in forms, giving social insurance numbers, or using credit cards. Second, it helps to constitute complementary selves for those subjects, the sum, as it were, of their transactions. New individuals are created who bear the same names but who are digitally shorn of their human ambiguities and whose personalities are built artificially from matched data. Artificial these may be, but these computer "selves" have a part to play in determining the

life-chances of their human namesakes. Thus are subjects constituted and deviants defined within the Superpanopticon.

Evaluating Electronic Panopticism

The Panopticon offers a powerful and compelling metaphor for understanding electronic surveillance. The prison-like society, where invisible observers track our digital footprints, does indeed seem panoptic. Bentham would surely smile wryly if he saw us complying with institutional norms as we use barcoded library books or note telephone callers' ID before accepting a call. The familiar distinctions between public and private life dissolve as both government and corporation ignore old thresholds and garner personal data of the most mundane and intimate kinds.

Beyond the metaphor, a model of power also lies in the concept of the Panopticon. The normalizing discipline, the exaggerated visibility of the subject, the unverifiability of observation, the subject as bearer of surveillance, the quest for factual certainty - all are important aspects of the Panopticon as a model of power. The question is, to what extent are all these necessarily present in each electronic context? Would the claim be sociologically warranted that electronic surveillance is panoptic power?

To answer this question satisfactorily, three others must be addressed. First, *can the Panopticon be generalized across different social spheres?* From the above discussion, it is evident that social analysts using the panoptic image think of electronic surveillance as a process that spills over conventional social boundaries. For example, we have seen how Zuboff's celebrated ethnography of computer-based technologies in the

workplace draws on the panoptic metaphor to show how managers maintain control. New technology renders workers' activities transparent to management, inducing conformity to a degree undreamed of two centuries ago, or even two decades ago (1988). Similarly, Gary Marx's analysis of American undercover police practices documents the emergence of a "new surveillance" based primarily on computer technology that is subtle, decentralized, and increasingly permeates society at large. Its lineage may be traced from the Panopticon, through the maximum security prison to the "maximum security society" (1988).

In a Canadian context, Vincent Mosco sees the Panopticon operating through the computerization of marketing techniques, a process that he and others refer to as "social management" (Mosco, 1989). What Foucault calls the "capillary level" of the social organism, that is, the minutiae of everyday life routines, is penetrated by the new surveillance. In parallel with commercial developments, of course, is the massive electronic enhancement of government data-collection practices. Rob Kling, for example, asks, "Have computerized information systems effectively transformed Bentham's panoptic principle from a strategy which is only feasible in village-scale settings to a routine means of mass surveillance by modern states?" (1986: 3).

As these examples demonstrate, the Panopticon has been applied to diverse social spheres, not all of which would normally be associated with each other. For Foucault, the Panopticon epitomizes the disciplinary network of social relations seen not only in prisons but in the capitalist enterprise, military organization, and in a multitude of state-run institutions. It does not wait for offenders to act, but classifies and situates before any

"event", producing not "good citizens" but a "docile, deviant population" (Dandeker, 1990: 27). Despite Foucault's opposition to what he calls "totalizing", he frequently gives the impression that the panoptic prison has been made redundant through the development of a disciplinary network on a societal level: the Panopticon-at-large. Analysts of electronic surveillance may be forgiven for picking up a relatively undifferentiated view of power from Foucault.

This view has not been without critics, among them Anthony Giddens. The nub of Giddens' criticism is that, one, we must differentiate between the means of economic production and the political means of administration and two, that prisons are qualitatively different from other social organizations. With respect to the first, the fact that, during the nineteenth century, locales were established in which regular observation of activity could take place with the purpose of control makes the workplace and the state similar, but not the same. According to Giddens, workplace subordination rests on a hidden exploitative relation, unlike the nation-state, which ultimately depends for its power on a monopoly of the "means of violence".

Regarding the nature of prisons, Giddens points out that inmates have to spend all their time there; they are what Goffman calls "total institutions". Contrast schools, business firms or other civil organizations, where only a part of the day is spent, and where disciplinary power is far more diffuse. Thus for Giddens: "Foucault is mistaken insofar as he regards 'maximized' disciplinary power of this sort [i.e. panoptic] as expressing the general nature of administrative power within the modern state" (1985: 185).

Giddens' critique is well taken, at least insofar as it touches on pre-electronic features of modern social institutions. Foucault, and his followers, do exaggerate the centrality of the Panopticon within the disciplinary apparatus of modernity. But perhaps just as Foucault was making a rhetorical point over and against those who would stress the humanitarian motives in founding early prisons, so today those who would characterize electronic surveillance as panoptic perhaps do so in a *salutary* fashion, over and against others who regard it as benign, or who believe that privacy laws offer adequate social safeguards for it or personal protection from it. Electronic technologies do seem to diffuse surveillance throughout society in new ways.

As I have shown, Giddens' neat theoretical distinctions do begin to blur when confronted with the realities of contemporary electronic surveillance. Increasingly, disciplinary networks *do* connect employment with civil status or consumption with policing. Moreover, the very processes of time-space distanciation so aptly analysed by Giddens may well be undergoing further alteration. Once, this characteristically modern geographical and temporal "stretching" of social relations was facilitated by changes in transport and communications (Innis, 1951). Now, the advent of information technologies enables novel configurations. The worker could once leave the capitalistic enterprise behind at the factory gates. Now it follows him or her home as a consumer. The same home was once regarded as a private haven. The computerized "king" may now enter the "Englishman's home" at will. Indeed, the householder carries him in, disguised as a social insurance number. The distinctions discussed by Giddens still retain their salience for much of society today, one suspects. It is an empirical question how long they will

continue to do so in the same ways as surveillance is progressively augmented by information technology.

Even if new technology does facilitate a novel penetration of the mundane routines of everyday life, however, it is not clear that this in itself augments a general societal panopticism. For Bentham and the other bearers of modernity have in a sense done their work. Citizens of the contemporary advanced societies are already expert-dependent in a radical sense. We cannot help but rely upon those "in the know," the experts (Bauman, 1991; Giddens, 1990). Equally, electronic panopticism may turn out to be a vestigial residue of modernity's - Benthamite - utopian hunger for certitude. The ghost of the unseen inspector may continue to haunt specific milieux, such as Zuboff's pulp mill, courtesy of computer-power. It may even contribute to new forms of categorizing subjects across different spheres and thus serve to sustain social control, but this still does not add up to the more apocalyptic vision of a societal Panopticon. Nonetheless, even such "panoptic residues" raise some significant social queries.

This discussion of historical changes and of consumerism in particular brings me to my second question; *does the Panopticon do justice to the realities of social order in capitalist societies*? Numerous plausible answers have been given to the classic sociological query of how social order is maintained. To be worth anything, the answer must connect directly with contemporary realities.

Today consumerism contributes heavily to the maintenance of social order; the Panopticon deals with those left out of the market. Zygmunt Bauman points to a duality between what he refers to as the "seduced" and the "repressed". People become socially

integrated - seduced - by means of market dependency. Though Bauman makes little reference to the fact, this is powered in part by commercial surveillance. But its strength does not lie in a panoptic "imposing of norms". Surveillance supplies a structure to channel behaviour, but one within which real choices are made.

Rather, social skills and economic capacity entitle the seduced majority to consume. Some panoptic methods may well underlie the surveillance techniques used to seduce. But the minority, the new poor or the underclass, is subjected to tight normative regulation, where the excluding capacities of the Panopticon come into their own. This would explain why modern life is experienced by the majority as pleasure and not - as the "social Panopticon" theorists see it - as a prison sentence. In fact, according to Clifford Shearing and Philip Stenning, a similar distinction is already present in the work of Foucault. They say he worked with both a generic concept of discipline and a more (fully worked out) "historically specific examination of it in the context of carceral punishment" (1985: 336).

Foucault's "physics or anatomy of power" represents the generic mode of discipline, of which the Panopticon is merely a type. Discipline is dispersed throughout the microrelations that constitute society. It is not, for Foucault, "from above", like monarchical power. This embeddedness of power, say Shearing and Stenning, is what makes the Panopticon the exemplar of discipline. They go on to contrast the *moral* discipline of carceral punishment - for example in the Panopticon - with the merely *instrumental* discipline manifest in other locations such as factories, hospitals or workshops. Their own investigation of private security and control companies in Canada

reveal a discipline that is strictly instrumental, not moral in basis. As they say, "Within private control the instrumental language of profit and loss replaces the moral language of criminal justice" (1985: 339-40).

The distinction between the moral "soul-training" of carceral discipline and the instrumental discipline of private security systems is a useful one, though how far it reflects what Foucault wanted to argue is debatable. Rather like Bauman, Shearing and Stenning see "the dominant force in social control" as consumption, visible in microcosm in Disneyworld. Less like Orwell's nightmare, much more like Huxley's *Brave New World*, here is consensually-based control in which "people are seduced into conformity by the pleasures offered by the drug 'soma' rather than coerced into compliance by the threat of Big Brother, just as people are today seduced to conform by the pleasures of consuming the goods that corporate power has to offer" (1985: 347).

Here then is a plausible answer to the question about the reproduction of social order in the capitalist societies of the late twentieth century. Paradoxically, the Panopticon may not be an appropriate image on account of its capacity to make "society like a prison" so much as because of the embedded nature of its discipline.[5] However, this does not mean that we can safely forget the Panopticon. Carceral discipline, perhaps relating to residual moral categories, may still well be experienced by Bauman's "repressed". But, as I have stressed above, this is a residual not a general, let alone an expanding category. It is here that we find most signs of the Panopticon as it appears in

---

[5] As well as embeddedness, other features noted by Shearing and Stenning remain significant for the analysis of consumer surveillance: it is preventative, cooperative, non-coercive, consensual, non-carceral, instrumental, and effective.

Foucault's *Discipline and Punish*. But as the repressed are frequently, as Bauman puts it, "flawed consumers", a question arises as to how far even the normative discipline meted out to them is actually moral and not merely instrumental. The norms from which they deviate are essentially rooted in consumer skills. It is primarily participation in society as consumers from which they are excluded, through lack of credit-worthiness, welfare dependence, and so on.

As it could be argued that the application of information technology encourages the extension of instrumental discipline, the question of whether this constitutes a dominant trend becomes even more pressing. The Lyotardian lament for the loss of the (moral) "metanarratives" of modernity and their replacement with the (instrumental) categories of computerized control (Lyotard, 1984) may become an increasingly important site for social investigation. If he is correct, perhaps Max Weber's worries about a completely "rationalized" world will turn out to have been justified.

The idea of a dual system of control raises further questions about political power, democratic institutions, and citizenship. This brings me to the third and final question I wish to address regarding the panoptic qualities of electronic surveillance. *Does the Panopticon yield a complete picture of the origins and nature of surveillance?* Of course this question has already received a partial - and negative - answer, but now I want to focus on the ambiguities or paradoxes of surveillance, and on what Giddens calls the "dialectic of control" (1985). This also involves looking not only at where Foucault obtained his conception of the Panopticon, but where Bentham got it in the first place.

We may grant that Foucault theorized a more general view of disciplinary power than that embodied in the Panopticon. But he certainly gave the impression that citizens of modern nation-states find themselves increasingly to be the subjects of centralized carceral discipline. And, for someone who spent precious little time considering how the warm "bodies" of which he wrote might *respond* to such discipline, he made a curious closing comment in *Discipline and Punish*; "In this central and centralized humanity, the effect and instrument of complex power relations, bodies, and forces subjected by multiple forces of 'incarceration', objects for discourses that are themselves elements for this strategy, we must hear the distant roar of battle (1979: 308).

It is not clear that the roar of battle was as loud as Foucault predicted, or so distant. If the "battle" is one of revolt against discipline, then this assumes, further, that discipline is viewed by subjects in an entirely negative light, and that there would be a considerable time-lag between the imposition of discipline and the battle. However, one could equally argue, on sound historical grounds, that changing processes of social control always occur in the context of struggle and that the contest is confused, ambiguous, and recursive.

Giddens generalizes this phenomenon in his "dialectic of control", in which all strategies of control "call forth counter-strategies on the part of subordinates" (1985: 11). Of course, Giddens hangs onto human agency here, a premise abandoned in Foucault's work. Giddens sees the build-up of administrative power as accompanied by expanding reciprocal relations between rules and ruled. Equally, he regards modern management practices as involving reciprocity. Strategies and counter-strategies are in constant tension

with each other. In this account, Foucault's battle is neither distant nor, necessarily roaring.

However, a further question raised by this chapter - and Part I of the dissertation - remains; does surveillance alter its character as information technology facilitates its further reach and efficiency? If, as I have suggested, the answer is yes, then how might this affect the dialectic of control, the Foucault paradox? Palpable social and personal benefits undoubtedly accompany the use of information technology in surveillance systems. Gary Marx, for instance, acknowledges that it is effective in apprehending criminals, detecting corruption, preventing crime, verifying arms control, and monitoring health (1988). Similarly, users of credit cards find them convenient and reliable; many are grateful for the ease with which shopping, banking or travel can be accomplished when using computer based equipment. As such, whatever the deeper consequences for the quality of life, none of the above is generally regarded as negative.

This idea connects with the historical rise of modernity noted in the previous chapter; the much-prized achievement of welfare citizenship in modern societies could only become effective if accompanied by the growth of a state bureaucracy capable of enforcing these rights in practice (Abercrombie et al, 1986: 179). In other words, the burgeoning panopticism of nineteenth century institutions emerged hand-in-hand with growing commitments to social rights. Recognizing people as unique identities to ensure that each is treated equally simultaneously makes their control that much easier.

Fears and anxieties about electronic surveillance, and critiques of or resistance to it, arise from specific aspects of its panoptic character. Opponents of the new surveillance

deplore the fact that it depends upon categories, that no knowledge of the individual is required, that it is increasingly instrumental, that areas of personal life once thought to be inviolably private are invaded, and that it effectively erodes personal and democratic freedoms. Foucault offers little help at this point, not only because he did not comment on computer technologies, but more profoundly, because he never examined the basis of his own "moral outrage" against the Panopticon (Jay, 1989).

Critics of electronic surveillance could do worse than to turn again to Bentham to define the object of their ire. After all, as Foucault rightly observed, Bentham's work does indeed mark a watershed in the understanding of social control. In the Panopticon, the issues are sharply etched. What contemporary commentators object to is both prefigured in the Panopticon and emphasized by the electronic. Bentham, following the Cartesian logic that regarded human beings as machines whose activities could be measured and controlled, wrote impersonality, abstract classification, and automatic power into the Panopticon. Precisely these features reappear, now digitally inscribed and intensified, in the new, computer-run surveillance.

Bentham's project was nothing less than a secular utopia, a model society-in-miniature, cut loose from any theological moorings that might complicate his claim that the Panopticon stood as the solution par excellence to the human condition (Crimmons, 1986; Strub, 1989). In the crucial principle of inspection, he explicitly parodied the doctrine of divine omniscience, taking it to be an unsurpassed means of moral control. What he conveniently ignored, though, was the personal character of knowledge present in the biblical quotations with which he ironically epigraphed his text. It is hardly

surprising, then, that the Panopticon excludes the personal, and slips almost imperceptibly from moral to instrumental categories. It is equally unremarkable, given this backdrop, that today's actors in the surveillance drama have started to focus their criticisms on these aspects of electronic panopticism - perceived control by inspection and categorization.

Towards an Alternative

The paradigms deriving from Orwell and Foucault are dystopian, containing notes of warning, doom-laden predictions, and conscious allusions such as those to Big Brother, watching. As such, they have the virtue of directing our attention to the negative, constraining, and unjust aspects of surveillance, and of helping us to identify trends that are especially dangerous from this point of view. But their disadvantage is that they may exaggerate the negative by seeing only one side of surveillance, promote pessimism about whether such negative traits can be countered, and fail to offer any indication as to what the content of an alternative might be. Herein lies the challenge for surveillance theory; to search for agency and the possibility of hope.

Both Big Brother and the Panopticon are used successfully as a means of highlighting what is negative about surveillance, but they leave unanswered the question of what sort of society is desirable, as far as surveillance is concerned. In this section, I try and clear some space for an alternative, or at least a complementary, approach by examining the categories of openness, accountability, and co-operation as discussed by Geoffrey Brown (1990). By sketching the contours of a new approach to surveillance, I suggest that common obstacles to appropriate political action might be removed. In other

words, attitudes and action would both be better informed if we had a clearer idea of what a desirable future might look like.

Geoffrey Brown proposes that controlling the circulation of personal information is a question of the appropriateness of disclosure within differing contexts (1990). Thus, "access to particular information is systematically related in the appropriate way to the network of social relationships in which that person stands to others by virtue of their place in the role structure" (1990: 77). In this view, breaches of privacy are attacks on the integrity of social identity. The sense of selfhood is diminished and freedom is constrained.

Of course, this approach raises numerous questions, for example, what if I don't accept some role assigned to me? But its advantage lies first, in the emphasis on modern surveillance itself, and not just the consequences, say, of inaccurate data being a potential threat, or at least something less desirable. Second, this kind of approach has much to offer those engaged in the law and policy making process. The question of personhood and social identity relates to the issue of how identity is negotiated, which in turn connects with the processes of human communication.

To understand surveillance in relation to social processes of communication opens new doors. To say that we form and maintain self-identity by means of negotiation reminds us of some important factors. For example, before the advent of modern surveillance systems, communicating the kind of personal data now required by such systems depended on particular sets of relationships. What might be reported to a doctor, confessed to a priest or admitted to a close friend depended on the nature and quality of a

given relationship. One might say certain things in one context but not in another. Given the commitments of certain professionals and kin to confidentiality, what was spoken to one would not be passed on to another. So personal data, in a world characterized by face-to-face relations, tends to be limited to voluntary disclosure to chosen confidants within relations of trust.

Of course, this could be seen as idealizing traditional situations and disregarding tendencies to gossip, slander, and engage in malicious whisper. But even to acknowledge these things is to note that such practices are considered undesirable. The social expectation, and indeed the very possibility of social intercourse, depends on the ongoing exercise of trust and tact. Although Goffman's work may be read as depicting the cynical manipulation of events and people by "actors" occupying temporary and maybe strategic roles, even there an underlying sense of mutual commitments and social collaboration is evident (Giddens, 1987). Today, in the world of abstract systems dependent on the manipulation of digital symbols, the idea that communicating personal information could be in the nature of voluntary disclosure of select items to specific persons tied to us by trust seems simply unfeasible.

But taking such a view of personhood seriously is not entirely anachronism. For example, the British Data Protection Act is based on the principles that "personal data shall be obtained and processed fairly and lawfully, held only for those purposes, and only be disclosed to [certain] people" (1984: 10). It provides for "individuals to have access to data held on themselves and, where necessary, have the data corrected or deleted" (1984: 10). So people can, in principle at least, know about data held about them and, if they

have the motivation, ensure that they are correct, up-to-date, and appropriate. Thus, Brown rightly concludes that the long term solution to the problems of surveillance lies in such areas as "openness, accountability, and co-operation" (1990: 142-44).

From such practices as openness, accountability, and co-operation could come some real alternatives to today's surveillance difficulties. Equally, the problem may be couched, perhaps more sociologically, in terms of *participation*, *personhood*, and *purposes*. From "participation" derive some alternatives to the exclusionary power of much surveillance, from "personhood" some criteria by which to judge the data-image, and from "purposes" an antidote to the self-augmenting development of surveillance technologies.

Participation

We saw in Chapter Two how the growth of surveillance may be traced in part to the expansion of citizenship. That is to say, increasingly full social participation became available to members of nation-states on the basis of established civil, political, economic, and social rights. The administration of such rights entailed the use of documentary identification and the construction of personal dossiers. Whatever constraints this imposes has to be understood in light of the enablement offered.

However, the language of new technologies, superimposed upon that of bureaucratic organization and the extension of surveillance into the consumer sphere, now threatens some of those rights, so that the equation of constraint and enablement is less easy. The revival of interest in "citizenship" as a central concept for both social analysts and political practice is to be welcomed in this respect. It both extends and updates

pursuits of the just society, with which surveillance is symbiotically intertwined; at the same time it connects to the contemporary quest for full social participation for marginalized and excluded groups.

Surveillance practices seem more and more to reinforce the social order of consumerism, through credit cards, ISDN telephone services, and so on, while simultaneously maintaining existing social divisions, especially those between consumers and non-consumers or those within the occupational structure and those cut off from it. To seek a "balance of interests" between "individuals" and corporations or the "state" thus seems hopelessly inadequate when the starting point is such an asymmetry of power. In light of this, David Lyon proposes that as far as public and corporate policy is concerned, the goal of maximum social participation could be sought by means such as regarding computer networks as common carriers (1992). Of course this flies in the face of current deregulation, but it is not necessarily unrealistically utopian to consider this option.[6] Its virtue would be to reduce the power of "social management" by finding a place for both consumer and non-consumer voices to be heard. For example, rather than focus on "the right of individuals to access personal information about themselves" (Privacy Act, sec. 1), privacy could be rethought in terms of the right of a society to require institutions using personal information to do so in a matter that respects the shared interests in that information. Similarly, David Lyon and Elia Zureik suggest that "within what will no doubt continue to be called privacy laws, the emphasis should be shifted away from mere

---

[6] It is proposed, for instance, by Kevin Wilson. See *Technologies of Control: The New Interactive Media for the Home*, Madison, WI: University of Wisconsin Press, 1988, p.157.

self-protection and towards placing a greater onus on data-gatherers to ensure that data is obtained fairly, in the demonstrably best interests of data-subjects, and used only for those purposes and with as much subject access as possible" (Lyon and Zureik, 1996: 13). At present, this may seem to have a ring of unreality to it, but this is only because privacy and data protection law is so notoriously subject-unfriendly, an issue which will be discussed in detail in Chapter Four.

Personhood

This is the corollary of participation and is closely articulated with it. The specific question that prompts concern here, and that is so central to all contemporary surveillance, is the data-image. The data-image crucially affects life-chances and also renders fragile one's very reputation (Gandy, 1993). Both a "good life" and a "good name" may be put in jeopardy by it. The data-image objectifies, is based almost entirely on a one-way transmission of information, and is redolent of stereotypical masculine traits, while its categories are clustered around observable behaviour alone. Furthermore, it may turn out to be a means of domination in ways as yet only dimly perceived.

What I mean by this is that our humanness itself, rather than just our life chances or good name, is increasingly defined in terms of the data-image. Who we are to the ubiquitous machine, the ubiquitous connection, is more significant than who we are to ourselves or to each other. So far from there being a distinctiveness to being human, whether rooted in Habermas' language or in the *imago dei*, humanness may be redefined by surveillance based powers, to which we are accountable.

These features reflect the quest for efficiency, productivity, accuracy, and predictability that are the hallmarks of contemporary surveillance. But no technical reasons exist why other features should not be present as well or instead. Caring and protective motifs, for instance, would be one area to be explored. And the data-image could also be constructed in such a way as to include intentionality, as well as more mechanical behaviour, and forgiveness, in that records would be erased when no longer needed. To achieve this, groups of professionals, from systems designers to quality controllers, would have to be involved (Smith, 1994).

Purposes

Underlying both previous principles - participation and personhood - is the assumption that the purposes of surveillance systems should be the constant subject of analytical scrutiny and political concern. This is so because of the ease with which such purposes may be subverted, obscured or replaced. The story of surveillance in modern societies is studded with references to bureaucratic augmentation and technocratic enlargement, each of which exhibits strong tendencies towards autonomy. That is to say, instrumentality - mastery - predominates.

The alternative here would be to identify, not some fixed and static "purposes" for appropriate surveillance, but rather some dynamic criteria for gauging their appropriateness. Given the overweening ambition that appears to have attended most surveillance schemes since the Panopticon, a concentration on *limits* would be apt here. Limits to knowledge, the seeking of specificity rather than omniscience, constitute the most obvious of these to me. But another limit, highly pertinent to an era in which the use

of new technologies is serving to blur the boundaries between previously discrete domains, would be a sphere-by-sphere check on surveillance operations. What may be ethically or politically unassailable in one social field is often inadmissible in another (Regan, 1995). This raises questions, again, for the data-image, and also about the extent to which data-subjects may control personal information about them.

Understanding Surveillance: Beyond Orwell, Bentham, and Foucault

The three categories of participation, personhood, and purposes are offered here as a contribution to finding direction for hope in an analytical field dominated by dystopic models and metaphors. They are intended as a means by which the normative content of surveillance theory may be weighed, and by which new theory may be devised. Beyond theory, such categories could find a role within political practice at both the policy and the movement/mobilization levels discussed in Part III. For example, with regards to the former, university and college accreditation in the United States now requires inclusion of "social and ethical issues of computing."[7] In Britain, the Open University's "Introduction to Information Technology" includes similar questions.

With regards to the latter, public awareness of surveillance issues could be raised through professional groups and organizations, especially those directly concerned with computing, information management, and so on. For instance, the Computer

---

[7] See, for instance, materials from the Research Center on Computing and Society at Southern Connecticut State University as well as the undergraduate textbook by Sara Baase, *A Gift of Fire: Social, Legal, and Ethical Issues in Computing*, Upper Saddle River, N.J.: Prentice-Hall Inc., 1997.

Professionals for Social Responsibility (CPSR) group had dramatic success in blocking the development of the Lotus "Household Marketplace" software in 1991. The software, which was to have been sold on CD-ROM disks, was capable of revealing the names, addresses, martial status, and estimated income of some eighty million Americans at the push of a button. Through computer networks, CPSR argued that limits should be placed on the expansion of consumer surveillance. Such actions fit in exactly with the criteria of participation, personhood, and purposes discussed above. Resisting the growth of electronic surveillance *per se* is a futile gesture. However, attempting to channel it in ethically and politically appropriate directions is socially much more *a propos*.

Thus, informed mobilization responses, coupled with legal and educative policy initiatives, should be welcomed. Our worst fears of surveillance will be realized much more easily in contexts where such complacent assumptions reign as that computerized efficiency equals progress or that privacy laws adequately protect citizens. Which brings me back to a central argument advanced in the dissertation. Surveillance is a central institutional area of contemporary societies, and as such calls for both responsible social analysis *and* political action. We will see in the remaining sections of the dissertation that, without doubt, legal, technical, and even educational remedies to the problems raised by surveillance are often inadequate. However, I have suggested in this section that analytical approaches tied to dystopic paradigms are equally problematic. Contemporary surveillance must be understood in light of changed circumstances, especially the growing centrality of consumption and the widespread adoption of information technologies. In this vein, I have argued that imaginative analysis, informed by constructively critical theory

based on notions of participation, personhood, and purposes, would not only go a long way in removing common obstacles to political action, but would also help to eschew Foucauldian fatalism and Orwellian paranoia. As such, it may be possible to face the future with realism and hope.

PART II

Chapter Four: Surveillance and Current Canadian Public Policy

Surveillance and Canadian Public Policy: Current Conditions

It was argued in Part I that privacy scholars must be familiar with both the history and sociology of the advanced industrialized state. In addition, understanding is required in the areas of: the bewildering variety of privacy invasive and privacy enhancing technologies; the vagaries of public opinion; the structure and behaviour of modern organization; the economics of information; and public policy. It is to the latter area that the dissertation now turns. By focusing on public policy, though, I am not suggesting that privacy scholars need just look at the content and effects of policies, or at the powers and activities of the agencies that implement those policies. It is a fundamental premise of the dissertation that in order to understand contemporary surveillance, we must engage with several different kinds of debate, and communicate across several different disciplinary areas. Personal information is pervasive. Privacy invasion is pervasive. Public policy is just one of many social forces that affects the conditions for privacy in the 1990s.

But it is a tremendously important force insofar as it helps to institutionalize the idea that surveillance should not be permitted to grow unimpeded. Of course, creating laws and policies equal to the realities of today's surveillance is another matter; most privacy laws are sieve-like and subject-unfriendly and many of the privacy codes in the Canadian private sector are purely voluntary, which is to say that there is no particular compulsion to comply with a code once it is adopted, other than ethical obligation. Nevertheless, weak laws and policies are better than none at all. Precedents for some protection are set that way, and the foundation for improvements laid.

In addition, public policy is important insofar as social, political, and cultural challenges to surveillance often strive for particular policy initiatives. For example, privacy scholars and activists have repeatedly called for data protection legislation in the private sector. This claim has been echoed by various groups such as Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, the Internet Society, and Privacy Rights Clearinghouse. Finally, there are instances of "mobilization responses" which stimulate policy action. For example, public outrage over the release of Judge Robert Bork's video rental list to a major newspaper in 1988 led to the passage of the *Video Privacy Protection Act*, commonly referred to as the Bork Bill.

In light of the significance of public policy, then, this chapter describes existing legislative and voluntary provisions for personal data protection in Canada. The first section provides a brief overview of the regulatory provisions currently in force that affect the collection, storage, processing, and disclosure of personal information. Canada is one of the few advanced industrialized states that has not passed comprehensive legislation governing the collection, use, and disclosure of personal information by *all* organizations. The public sector is relatively well regulated through the 1982 Privacy Act and corresponding provincial statutes. But, with the exception of *An Act Respecting the Protection of Personal Information in The Private Sector* (Bill 68) in Quebec, privacy protection in the private sector in the rest of Canada has emerged in an incremental and piecemeal fashion.

Most provinces have statutes protecting the collection, use, and disclosure of credit-reporting information. The new Telecommunications Act (Bill 62) empowers the

Canadian Radio-Television and Telecommunications Commission (CRTC) to regulate to protect privacy interests. In addition, there exists a number of confidentiality provisions for personal information within other federal and provincial laws. However, the overall legislative profile for Canadian personal data protection has been likened to a "patchwork". This incoherence is confusing to the consumer, potentially damaging to business, and inadequate to meet emerging international standards for personal data transfer.

The principal response in most sectors has been to develop "voluntary" privacy codes of practice. However, the term "privacy code" describes a diversity of mechanisms. In the second section of the chapter, five types are identified: *Individual Company Codes*; *Sectoral Codes*; *Functional Codes*; *Technological Codes*; and *Professional Codes*. These codes vary according to their scope of application and their extent of compulsion. Most operate within a complicated and fluctuating range of regulatory, technological, cultural, and business incentives. The term "voluntary" needs to be used with considerable caution.

An analysis of the major privacy codes in the third and final section bears out these differences. For example, the "Sectoral Codes" of the Canadian Bankers Association, the Canadian Life and Health Insurance Association, the Insurance Bureau of Canada, and Stentor are models designed by these trade associations for the membership to implement at the company level. On the other hand, the "Functional Code" of the Canadian Direct Marketing Association gives the association a greater role in mediating complaints and promoting consumer awareness, with a threat of expulsion of a member company for non-compliance. Finally, the privacy policy of the cable television industry operates according

to a *foundation model*, under which the Canadian Cable Television Standards Council administers cable television service contracts, including privacy, under the oversight of the CRTC.

The three sections outlined above are intended to provide some context for the discussion of the background conditions and short term events that are making policy change possible at the level of the federal government. These conditions and events, which are examined in Chapter Five, provide a short term answer to the first question proposed in the dissertation: why is privacy legislation for the private sector "an idea whose time has come" in this country?

In addition, the three sections are intended to provide some context for the analysis of mobilization movements. In this regard, I suggest that despite the necessity for privacy laws, what can be achieved by these measures is chronically limited, not only in the sense that such measures may be "too little, too late" but also in the sense that the law itself is inadequate to the task of regulating electronic surveillance. Social, political, and cultural approaches, though less tangible, may be more appropriate. These approaches, to be examined in Part III, provide some answers to the second question proposed in the dissertation: how can public awareness about surveillance be increased?

Finally, the research methodology for this chapter has involved the following activities. First, a substantial amount of documentary evidence has been collected and analysed. This includes regulations, codes of practice, guidance notes, promotional materials, training manuals, and so on. Second, non-structured interviews have been conducted with representatives from a range of public and private organizations in

Canada, including trade associations, the offices of Information and Privacy Commissioners, offices of other federal agencies, consumer associations and public interest groups, and experts in auditing, management information systems, and computer security. A list of the agencies and organizations contacted is included in the Appendix. Lastly, I have drawn upon the secondary literature on privacy and data protection in North America and Europe. In this regard, it is important to note that while there is a large number of books and articles on privacy and data protection laws, there is, curiously, very little on codes of practice. I am hopeful, therefore, that this research will help to fill a longstanding gap in the literature on privacy and data protection.

The Regulatory Environment for Personal Data Protection in Canada

I. Public Sector Practices

The second world war had a major impact on the landscape of human rights, and in particular, the right to privacy. Three important international human rights documents were promulgated after the war, and all include guarantees of the right to privacy. The *Universal Declaration of Human Rights* was created in 1948, Article 12 of which contains the provision that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation". The same provision was included as Article 17 of the *International Covenant on Civil and Political Rights* in 1966, to which Canada acceded in 1976. In 1950, the *European Convention for the Protection of Human Rights and Fundamental Freedoms*

was created, Article 8 of which states that "Everyone has the right to respect for his private and family life, his home, and his correspondence".

The development of the computer in the 1960s and 1970s led to concern in Europe that the privacy provision in the European Convention was no longer adequate. In 1980, the Council of Europe thereby enacted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. This Convention contains the original framework for most modern data protection laws: personal data should be obtained and processed fairly and lawfully; data should be stored for specific and legitimate purposes, and not used for any other purposes; data should be relevant, adequate, and not excessive for the purposes at hand; data should be accurate, and up to date; and data should be kept for no longer than is required for the original purpose. The Convention sets out rights of access and correction, and required member states to enact laws providing for appropriate sanctions and remedies for violation of these principles.

At the same time, the Organization for Economic Cooperation and Development (OECD) became concerned that the development of domestic privacy and data protection laws would interfere with the free flow of information essential to international trade and economic development. The OECD therefore published *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* a few days following the promulgation of the Council of Europe's Convention in 1980. The objective of the Guidelines is primarily to prevent barriers to the free flow of information between member countries as a result of data protection efforts, while also ensuring observance by member states of appropriate data protection principles. The Council of the OECD recommended that

member countries take the Guidelines into account in drafting domestic legislation. At the heart of the Guidelines are eight "Basic Principles of National Application":

1. Collection Limitation Principle

Limited to the collection of personal data; data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, be accurate, complete, and kept up to date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified except: (a) with the consent of the data subject or (b) by the authority of the law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss of unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him

(b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him

(c) to be given reasons if a request under subparagraphs (a) and (b) is denied, and to be able to challenge a denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

At first glance, these principles seem like common sense. However, the methods chosen to implement them and the scope of their application vary widely among the member countries. For example, James Rule has demonstrated how U.S. legislation, ostensibly designed to curtail abusive information practices, has instead tended to

legitimate them. Regarding the *Fair Credit Reporting Act*, he states: "It is the genius of American liberalism that, when faced with a particularly unconscionable practice by some powerful interest, it regulates that interest in such a way as both to mitigate the sting of the abuse and at the same time to consolidate the position of the perpetrators" (1970: 214). Similarly, the Privacy Protection Study Commission, evaluating the U.S. Privacy Act of 1974, concluded that it was more admirable for its apparent "spirit" - which had been universally ignored by the federal bureaucracy - than for any contribution it had made to the restriction of information practices (1977: 499, 532).

Writing in a more critical vein, Kevin Wilson has argued that the impact of privacy legislation in Canada has not been to curtail the collection, use or exchange of personal data. Rather, legislation seeks to regularize the surveillance practices of bureaucracies by sanctioning "routine" collection, use, and disclosure (Wilson, 1988: 78). For example, Wilson notes that the principal function of access provisions is not to redress or affect the balance of power between individual and institution in any real sense. Instead, these clauses are designed to ensure that decision making based on personal files is founded on "accurate" information and also to reassure the client about the fairness of institutional processing of his or her file. According to the Canadian Privacy Act (12 (1)):

> Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of the *Immigration Act*, 1976, has a right to and shall, on request, be given access to: (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it retrievable by the government institution.

Thus, the Act establishes procedures for the processing of access requests by clients and creates rules for institutional response (13(1), (2); 14). As such, individuals get some measure of control over their personal data. However, on a societal level, privacy legislation in North America fails to jeopardize a fundamental category of corporate control administered through forms of public surveillance.

II. Private Sector Practices

One of the chief criticisms of North American privacy legislation is that it fails to cover both the public and private sectors. In the United States, this has been a matter of quite conscious policy. For instance, the United States Privacy Protection Committee that reported in 1977 explicitly rejected an omnibus private sector data protection law on the European model in favour of a combination of legislation and non-statutory codes that would be sector-specific and, arguably, more sensitive to the different information handling practices and needs of different industries. In Canada, there has never been an authoritative analysis of private sector data protection issues. Controls have, therefore, emerged in an incremental manner as pressures from developments in information technology, from international organizations, and also from public opinion have forced some sectors of the Canadian economy to grapple with the issue.

What follows in the remainder of this section is a brief inventory of the most recent statutory data protection provisions that are relevant to the collection, storage, and dissemination of personal data by the private sector in Canada. It is important to note, however, that where the "public" sector ends and the "private" sector begins is becoming increasingly difficult to determine. The British Columbia privacy legislation, for example,

pushes the boundaries of the public sector further than anywhere else in Canada, by including the "self-governing" professions and hospitals within its scope.[8] In addition, it was noted in Part I that there is an increasing tendency for the sharing, matching, and trading of government information as new service-delivery options are contracted out to private organizations.

The analysis also excludes from consideration common law restrictions on invasions of privacy, which have implications for practices like video surveillance and wiretapping. Suffice it to say that there is limited protection in common law for the infringement of one's privacy, mainly because Canadian courts have occasionally been able to find liability under associated torts such as trespass, nuisance, defamation or breach of confidence.[9] The analysis also excludes the emerging, though limited, privacy rights that the courts have found within sections 1 and 8 of the Charter.[10] However, that still leaves a range of relevant provisions to consider: Quebec's Bill 68, the provincial credit legislation, and recent enactments within the field of telecommunications.

(1) Quebec's Bill 68

---

[8] British Columbia, *Freedom of Information and Protection of Privacy Act of 1992*, S.B.C. 1992, c. 61. These institutions are covered under the "second tier" amendments that came into effect in November 1994.

[9] In only one case has a court found a right of recovery on the basis of a general right to privacy. In Saccone v. Orr the plaintiff successfully sued the defendant for taping and broadcasting a telephone conversation without consent [(1981), 34 O.R. (2nd) 317 (Co.Ct)].

[10] The Federal Privacy Commissioner, Bruce Philips, has pressed for an entrenched Charter right to personal privacy. See Privacy Commissioner of Canada, *Entrenching a Constitutional Right to Privacy for Canadians: A Background Paper*, Ottawa: Office of Privacy Commissioner, 1992.

By far the most significant development in the area of information privacy in the private sector has been the enactment, in 1993, of Quebec's Bill 68, *An Act Respecting the Protection of Personal Information in The Private Sector*. Bill 68 actually establishes no new rights, but it gives effect to the information privacy rights incorporated in Sections 34-41 of the new Civil Code. The law came into effect in January 1994. Quebec has thus enacted the first comprehensive regulation of private sector personal data practices anywhere in North America.

Bill 68 incorporates the fair information principles in the OECD Guidelines, supplemented by certain key provisions from the latest draft of the EU Directive. As such, it places restrictions on the collection of personal information and obliges organizations to protect the confidentiality of those data. Additionally, Bill 68 requires that communication to third parties beyond that mentioned at the time of collection may only be made if the individual has given "manifest, free, and enlightened" consent, although a number of exemptions are also provided to this provision. Upon request, individuals are entitled to receive confirmation of the existence of a file about them, as well as rights of access and rectification.

Bill 68 applies to all pieces of personal information collected, held, used or distributed by another person, confined mainly to enterprises engaged in an "organized economic activity". Thus, it excludes information collected for personal or family reasons - for example, an address or phone list. The bill singles out "personal information agents", chiefly credit bureaus, as a special type of enterprise. These are expected to register with

the Access to Information Commission (CAI), the body established under the 1982 public sector access and privacy law.

The CAI is also responsible for hearing complaints and can render binding decisions, ranging from a *mandamus* to an order that an activity be ceased. It may investigate any matter brought to its attention by a complaint, and it has wide powers to enter premises and examine information. The Quebec Commissioner also has powers to prevent the flow of personal data to parties outside Quebec, if that information will be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned.

The implications of Bill 68 are far-reaching. At the moment, Canada is the only country in which the scope of privacy protection in one of its jurisdictions exceeds that of the federal government. Within the province, there is initial evidence that the Bill has promoted a greater desire on the part of businesses to be seen to be promoting privacy-friendly practices. In the rest of Canada, it has prompted some enterprises within the federally regulated private sector - for example, the banks and the airlines - to declare their willingness to abide by the legislation, even though the wider jurisdictional issues remain unresolved. Thus, Bill 68 has further highlighted the "patchwork" nature of Canadian privacy protection as well as the diversity and incoherence of privacy standards in this country.

(2) Consumer Credit Legislation

The industry that has had the longest experience of having to comply with data protection rules in Canada is the consumer credit industry - including all those

organizations that collect and provide credit information for the benefit of merchants. Personal information is both the "foundation of the credit industry and its principal by-product" (Lawson, 1992: 11). Credit reports are compiled principally from information provided by the credit granters themselves. More controversial has been that gleaned from third party sources, such as court and municipal records.

From an early stage in the privacy debate, the potential harm that could arise from the use of erroneous information in these files was clearly recognized by both privacy advocates and the industry. Several countries, including the United States and Britain, enacted national consumer credit legislation in the early 1970s as a way to ensure consumer rights and to protect the integrity of the credit-checking and credit-granting process. In Canada, the industry regulated at the provincial level. All English-speaking provinces except Alberta and New Brunswick now have legislation aimed at controlling the collection, use, and disclosure of personal information that is intended to be used by third parties for the determination of credit-worthiness.[11] In Quebec, the industry is regulated through Bill 68.

Consumer credit laws attempt to regulate what is reported, to whom, and for how long. They prohibit anyone from acting as a credit reporter unless registered with or licensed by a body such as the *Registrar of Consumer Reporting* in Ontario. The license renewal process generally permits questions to be asked and audits to be conducted.

---

[11] Ontario, *Consumer Reporting Act*, R.S.O. 1990, c. C.33; B.C., *Credit Reporting Act*, R.S.B.C. 1979, c.78; Manitoba, *Personal Investigations Act*, S.C. 1971. c.23; Saskatchewan, *Credit Reporting Agencies Act*, R.S.S. 1978, c. C-44; Nova Scotia, *Consumer Reporting Act*, R.S.P.E.I. 1974, c. C-18; Newfoundland, *Consumer Reporting Agencies Act*, S.N. 1977, c.18.

Credit reporters are typically prohibited from releasing information to anyone except those intending to extend credit or collect a debt. They are expected to ensure data accuracy and timeliness through retention schedules, which are normally six years. Some laws also prohibit the collection of sensitive information relating to race, creed, colour, sex, ancestry, ethnic origin or political affiliation. They also prohibit the seeking of a credit report on a person unless that person has first been notified in writing, normally at the time of application for credit, though there is dispute as to whether this constitutes "consent". Most laws impose criminal sanctions and/or civil remedies for violation of the provisions.

There is an ongoing debate about whether consumer credit laws provide effective mechanisms for the protection of consumer privacy and whether they have been overtaken by technological progress. Kevin Wilson, for instance, suggests that consumer credit legislation does not effectively constrain the collection of personal information by credit bureaus, let alone by credit grantors, employers, or insurers (1988: 75). For instance, the laws do not question the extent to which information gathered in the context of these relationships may be used for purposes other than those concerning consumer eligibility. Information collected in conjunction with credit, insurance, or employment relationships may be applied to operational or marketing decisions essential to the stability and adaptability of an organization; such information may have nothing to do with consumer eligibility, but the consumer is unaware of this. Thus, consumer credit legislation fails to reduce the collection of personal data to any significant degree (Wilson, 1988: 65). As such, it fail to address the importance of expanding corporate power and the role played by personal documentation in this expansion.

(3) Telecommunications Privacy

The other major sector in which privacy protection has been legislated is the area of telecommunications. In December 1992, the then Minister of Communications, Perrin Beatty, published a set of "Telecommunications Privacy Principles", in response to growing concern over the invasive nature of certain new telecommunications services and devices such as Caller ID, call-waiting, and cellular telephones.[12] Six principles were enunciated:

1. Canadians value their privacy. Personal privacy considerations must be addressed explicitly in the provision, use, and regulation of telecommunications services.
2. Canadians need to know the implications of the use of telecommunications services for their personal privacy. All providers of telecommunications services and government have a responsibility to communicate this information in an understandable and accessible form.
3. When telecommunications services that compromise personal privacy are introduced, appropriate measures must be taken to maintain the consumer's privacy at no extra cost, unless there are compelling reasons for not doing so.
4. It is fundamental to privacy that there be limits to the collection, use, and disclosure of personal information obtained by service providers and generated by telecommunications networks. Except where clearly in the public interest,

---

[12] Communications Canada, *Telecommunications Privacy Principles*, Ottawa: Minister of Supply and Services Canada, 1992.

or as authorized by law, such information should be collected, used, and disclosed only with the express and informed consent of the persons involved.

5. Fundamental to privacy is the right to be left alone. A balance should be struck between the legitimate use of unsolicited telecommunications and their potential for intrusion into personal privacy. All parties have a responsibility to establish ground rules and methods of redress so that Canadians are able to protect themselves from unwanted and intrusive telecommunications.

6. Privacy expectations of Canadians may change over time. Methods of protecting telecommunications privacy must be reviewed from time to time to meet these changing expectations and to respond to changing technologies and services.

The promulgation of these principles precipitated an interesting debate about their most effective implementation, a debate that suggests the various options that might be considered for the more general implementation of private sector data protection.[13] The Department of Communications considered voluntary acceptance, regulation through the CRTC, enforcement through the Telecommunications Act (Bill 62), new sectoral privacy legislation, and a model of joint regulation. They chose the last option and established a Telecommunications Privacy Protection Agency (TPPA) made up of representatives from industry and consumer groups. Funded through an industry foundation, the TPPA was responsible for enforcing the privacy principles, investigating complaints, and making certain binding decisions against businesses that flagrantly contravened the principles. For

---

[13] Department of Communications, *Privacy Principles Implementation Models*, December 22, 1992.

a number of political and practical reasons, however, the TPPA was never made fully operational. Its activities have been put on hold pending reaction to the *Model Code for the Protection of Personal Information* developed by the Canadian Standards Association (CSA).

To some extent, also, the TPPA was overtaken by other legislative developments, especially the enactment of the Telecommunications Act (Bill 62), which gave certain powers to the CRTC to "respond to the economic and social requirements of users of telecommunications services, including the protection of the privacy of individuals".[14] The simultaneous interpretation by Communications Canada was that this legislation explicitly granted the Commission the power to regulate to protect privacy interests. Thus far, the CRTC's most significant decisions in this area concern call management services[15] and Announcing Devices (ADADs).[16] In addition, 1993 legislation to protect the privacy of cellular telephone calls responded to mounting concerns about the ease of interception from commercially available scanners.

Important progress has been made, then, in the area of telecommunications privacy. However, it is important to recognize that there is no overall legislation in this sector that encompasses all the fair information principles. Current legislation regulates the introduction and use of telecommunications technologies and services in order to

---

[14] Bill C-62, *Telecommunications Act*, s. 7(h).

[15] CRTC, *Call Management Service - Blocking of Calling Number Identification*, Telecom Decision CRTC 92-7, May 4, 1992.

[16] CRTC, *Use of Telephone Company Facilities for the Provision of Unsolicited Telecommunications*, Telecom Decision CRTC 94-10, June 13, 1994.

minimize surveillance. But it does not encompass the full range of responsibilities and rights that are embedded in new policy initiatives such as the *Model Code for the Protection of Personal Information* from the CSA. Telecommunications privacy is thus largely dependent on the willingness and ability of the CRTC to interpret its mandate widely.

III. Comprehensive Versus Sectoral Data Protection

No doubt a complex array of federal and provincial statutory provisions other than the ones surveyed in the preceding section have a bearing on the collection, storage, processing, and confidentiality of personal information in Canada's private sector. The new *Bank Act*, for instance, allows the Governor in Council to make regulations "governing the use by a bank of any information supplied to the bank by its customers".[17] Other powers regulating the confidentiality of personal financial information are found in associated regulations and certain provincial statutes.[18] Legal provisions governing consumer protection, debt collection, patents, trademarks, and copyrights may also have limited relevance.[19] None of these, however, embraces the full range of fair information principles found under Quebec's Bill 68.

Thus, the overall regulatory picture in Canada is disparate and inconsistent. The approach in Quebec has been to follow the European model of a comprehensive

---

[17] *Bank Act*, S.C. 1991, c.46, S. 459.

[18] See Ian Lawson, *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*, Ottawa: Public Interest Advocacy Centre, 1992, p. 109.

[19] Ibid, pp. 107-14.

"omnibus" data protection statute. The approach in English Canada is one of incremental policy making on a sector-by-sector basis. In Quebec, the policy is more anticipatory of future data protection issues. In the rest of the country, the approach has been more reactive. Finally, in Quebec, the responsibility for oversight of data protection is almost totally within the remit of the CAI. In the other provinces, a range of regulatory bodies at provincial and federal levels, in addition to the offices of the Information and Privacy Commissioners, have potential oversight obligations.

The correct approach to personal data protection in Canada, then, is dependent on whether one favours comprehensive or sectoral data protection. Each of these approaches has particular advantages and drawbacks. One advantage of comprehensive regulation is that it allows for an adaptability to technological and economic change. However, privacy scholars from various backgrounds are now beginning to question whether the fair information principles inherent to comprehensive legislation are equal to the challenges of today's "information highway" environment. On the other hand, sector specific provisions are, arguably, more sensitive to the information processing needs of different sectors. A weakness of the sectoral approach, though, is that it is becoming increasingly difficult to determine where one sector begins and another ends. This problem is exacerbated by, for example, the convergence of the computer and telecommunications industries, the trend towards cross-ownership, and the globalization of the information economy. At present, it remains to be seen which approach will best meet the needs of the advanced industrialized states as well as which approach will be favoured by the federal government in its adoption of framework legislation for the Canadian private sector.

Voluntary Data Protection in Canada

I. What Are Privacy Codes?

The argument over the correct approach to personal data protection in Canada is compounded by the existence of numerous codes of practice, which have become prevalent not only in the field of privacy and data protection, but in many other areas of business activity as well. Codes of practice can provide a useful means of publicizing corporate practices, of reminding employees of their obligations, and of reassuring consumers. Within the data protection area, their utility has been recognized from the outset of the privacy debate in the 1970s.[20] As the need to develop sectorally specific regulation has grown, so their development and use has spread.

The instruments that have been called "privacy codes" are, however, extremely diverse. A recent report from the OECD concludes that "the term has become so entrenched into the data protection lexicon that it has come to be used to describe any attempt at self-regulation which appears in written form."[21] Similarly, a recent Guidance Note from the New Zealand Privacy Commissioner remarks: [22]

> The term 'code of practice' is used by different organizations in many different ways and covers varying levels of policy and practice. Codes of practice in other

---

[20] One of the early reports in Britain, for example, recommended a general system of data protection founded on the negotiation of codes that would subsequently be given statutory force. Great Britain, *Report of the Committee on Data Protection*, Cmnd. 7341, The Lindop Committee, London: HMSO, 1978 .

[21] OECD, *Privacy and Data Protection: Issues and Challenges*, Paris: OECD: Information Computer Communications Policy, 1994, p. 39.

[22] New Zealand Privacy Commissioner, *Draft Guidance Note on Codes of Practice under the Privacy Act*, Auckland: Privacy Commissioner, April 1993, p. 1.

> contexts can range from internal guidelines at one extreme to fully enforceable standards at the other. The term will continue to mean different things to different people in different contexts.

Thus, there is no commonly agreed-upon definition of privacy codes. As such, the analytical problem in this section is to outline the range of voluntary or self-regulatory instruments that currently exist in Canada and to determine the motivations for developing them. The motivations for the development of codes can substantially influence their content. To this end, I categorize the privacy codes according to two different factors: their scope of application and the extent to which they are "voluntary". This provides a general picture of where the gaps and overlaps exist.

II. Privacy Codes in Canada: The Scope of Application

Most codes of practice apply to private enterprises. As such, the subsequent analysis focuses on private sector instruments. In Canada, these can be categorized under five headings according to the scope of their application and the extent to which they are voluntary: *Individual Company Codes*; *Sectoral Codes*; *Functional Codes*; *Technological Codes*; and *Professional Codes*. It is worth noting, however, that other countries with general data protection legislation have seen an equally pressing need to develop codes for certain public sector practices. The first code negotiated under the New Zealand law, for instance, concerned health privacy.[23] The Council of Europe has also issued a number of "Recommendations" for the specific application of data protection rules, some of which

---

[23] New Zealand Privacy Commissioner, *Health Privacy Code 1994*, Auckland: Privacy Commissioner of New Zealand, 1994.

also apply to public sector practices. In general, though, specific applications in public sector agencies have been communicated through internal manuals and guidance notes.

(1) Individual Company Codes

A number of codes of practice have been developed by individual companies in the absence of, or in anticipation of, the development of wider sectoral instruments. Typically, these codes have been developed by large, high-profile organizations whose practices have come under scrutiny from the media and privacy advocates, and who may have received a large volume of customer complaints. Some have also developed policies as a result of consumer surveys.

The code produced by American Express is a notable example. The company's Director of International Consumer Affairs, James E. Tobin, reported in 1990 that "one of the greatest, if not *the* greatest concern at American Express these days is privacy. What worries us is that the industry is facing a major crisis of consumer confidence".[24] The latest version of the American Express Company *Privacy Code of Conduct* was published as a separate statement of policy in 1991 and applies to both customers and employees.[25] It was later supplemented by wider mailings to American Express Cardmembers, which allowed members to opt-out of receiving further information about promotional offers by

---

[24] James E. Tobin, "Privacy as a Bottom-Line Business Issue at American Express", Address to the Issues Management Association of Canada Conference, Ottawa, January 22, 1990.

[25] American Express, *The American Express Consumer Privacy Principles*, January 1991.

returning a postage-paid mailer or by calling a 1-800 number.[26] Initiatives by individual companies are, however, an exception. In most sectors in Canada privacy codes have been negotiated on a sectoral level, recognizing the need for a consistency of policy and practice, and the fact that most firms do not have the staff or financial resources to devote to this issue that American Express does.

(2) Sectoral Codes

Most company policies have, therefore, been developed within the framework of an already negotiated code of practice within a sectoral or group framework. This includes the banking, life and property insurance, telecommunications, and cable television industries. The specific provisions of these codes are discussed in greater detail in the next section. Some general remarks about sectoral codes are in order at this stage, however.

First, the major defining characteristic of sectoral codes is that there is a broad consonance of economic interest and function. By extension, there is also a broad similarity in the kinds of personal information that is collected and processed. Sectoral codes thus permit a more refined set of rules tailored more specifically to the problems of each industry.

Second, each of these sectors operates within an already-defined set of regulatory institutions and rules, most of which predate the rise of privacy to the national and political agenda. The sectors are thus given a certain pre-defined character by the regulatory environment. This in turn has established in each area a relatively cohesive

---

[26] American Express, "An Important Message to our Cardmembers concerning Privacy," 1993.

"policy community" that is engaged on an ongoing basis in the negotiation of new rules for the industry and in the implementation of existing rules.

Third, and finally, the trade associations that represent industry sectors vary in their representativeness. Some can claim to represent, and thus influence, the vast majority of companies that engage in that activity; the Canadian Bankers Association and the Canadian Cable Television Association fall within this category. In others, there are clearly players that operate outside; the resellers of long distance telephone services, for instance, are not represented by the Stentor organization.

(3) Functional Codes

What I call "functional" codes are defined less by the economic sector and more by the practice in which the organization is engaged. The most obvious example of this is direct mail and telemarketing, the operations of which have long raised privacy concern (Gandy, 1993). In Canada, the Canadian Direct Marketing Association (CDMA) includes representatives from almost every economic sector: retail, banking, insurance, transportation, telecommunications, and so on. Direct marketing is a huge industry, as noted in Chapter Three. The collection, processing, profiling, and matching of transactional data in order to target consumers for particular promotional campaigns is the life-blood of the industry. Thus, privacy and confidentiality rules are necessary not only to allay consumer suspicions but also to ensure the continued viability of the companies that provide listbroker services. The specific implementation mechanisms that the CDMA code employs are discussed in the next section.

(4) Technological Codes

Direct marketing is not the only "function" that may be amenable to privacy rules. A range of other practices, spanning all sectors, may also be governed through these means. To date, however, the only code that falls within this category is that adopted in 1992 by the banks for the governance of electronic funds transfer (EFT). This is a general code that attempts to regulate the issuance of debit cards and Personal Identification Numbers (PINs), the content of agreements between the issuer of the card and the cardholder, the nature of transaction records and statements, and security issues. The code also establishes a recommended dispute resolution process.[27] Thus, the code is concerned with many issues that extend beyond privacy and security.

(5) Professional Codes

The final category of privacy codes includes those that have been developed for use by professional societies. These impose or recommend obligations for employees in many different public and private organizations. Typically, these codes apply to those engaged directly in information processing activities. A steady development of professional codes and guidelines that include privacy and security provisions can have an important effect on the sense of professional responsibility shared by those in the frontline of information processing activity.

---

[27] Electronic Funds Transfer Working Group, *Canadian Code of Practice for Consumer Debit Card Services*, May 1, 1992.

The best Canadian example of this is the code developed by the Canadian Information Processing Society (CIPS).[28] CIPS, with over five thousand members, is the largest association in Canada representing information processing professionals. The CIPS code, circulated in 1988, was developed over seven years by a privacy working group that surveyed much of the literature and thought through several of the problems associated with organizational and individual responsibilities for personal data protection. Unfortunately, though, the CIPS code is little known and there has been no subsequent follow-up to measure compliance.

III. Privacy Codes in Canada: The Extent of Compulsion

The debate about personal privacy protection for the private sector is often couched as a choice between "voluntary" codes and legislation. This is a false dichotomy. The possible incentives for compliance fall along a complicated continuum. At one end is the purely voluntary code, in which there is neither internal nor external compulsion to develop, adopt or implement privacy standards. At the other, is the code that exists within a full set of statutory obligations and liabilities. Somewhere in the middle of this continuum fall most of the codes in Canada, where a complicated and fluctuating range of incentives and sanctions are continuously in play. The codes that fall between these extremes are often described as examples of "self-regulation". It is more important to make sense of this range of incentives than to argue about the correct labels.

---

[28] Canadian Information Processing Society, *The Protection of Privacy in Information Systems*, Toronto: CIPS, May 1988.

At the compulsory end of the continuum are those codes that give effect to existing data protection legislation. When a statutory framework exists, codes then tend to be interpretive instruments designed to apply these rules to specific industry practices and to inform employees of their obligations. They therefore tend to be quite detailed. In Canada, the only industry that falls into this category is the consumer credit industry, where the rules for access and correction, consent and notification, data security, retention schedules, and collection limitations are established under provincial consumer credit laws.

Other incentives are provided not by government regulation but by the imminence of regulation. This is often enough to prompt industry associations to engage in efforts at self-regulation. The circulation and debate of draft regulations can have such an impact. So can reminders to industry of the existence of regulatory powers that have been little used. The Privacy Commissioner of Canada has also played an active role in promoting self-regulatory activity through moral suasion.

The threat of expulsion from a trade association for not complying with a stated industry code of practice may also provide incentives for compliance. This threat is proportionate to the percentage of the industry that the trade association can claim to represent. The public isolation and exposure of one recalcitrant member is more likely to provide a plausible sanction the more comprehensive the association's membership. Expulsion can occur only when the association has the authority to carry out such an action, and when the recalcitrant member is not a large corporation on whom the association relies for substantial financial contributions. The structure of the industry and

the regulatory context are the principal factors that determine the credibility and likelihood of this sanction.

More subtle pressures may also come, however, from what can only be described as an organizational "culture" - that set of informal and unwritten norms that have evolved over time within industries, companies or professions. This factor is impossible to gauge definitively. It varies between and within organizations. Standards for data security and confidentiality, for example, in industries such as banking and insurance have long been recognized. These obligations are enforced as much through an informal ethos as they are through the written code of practice. Jeff Smith, in a recent analysis of private sector privacy protection in the United States, has also made a useful distinction between organizations that have a "strong culture of compliance", which typically choose a more rigid set of mechanisms, and those that adopt a "culture of commitment" based on "more flexible assumptions" (1994: 229).

Underlying this whole discussion about the level of compulsion for data protection rules is the elusive influence of market forces. It is now clear, for some industries at least, that the pursuit of "privacy-friendly" practices is also good business practice. As Alan Westin has noted, "Updated information privacy and security policies can increase the efficiency and effectiveness of consumer services, garner favourable media treatment, win goodwill from existing and potential customers, and enhance the company's reputation for social responsibility" (1991: 34).

Thus, voluntary codes operate with a complicated and fluid set of statutory, non-statutory, sectoral, cultural, and business incentives. These factors are not mutually

exclusive. Nor can they be arranged and compared in any definitive way across industry sectors. "Compliance" with data protection rules is dependent on the correspondence of these forces with wider technological and economic factors. That compliance will then vary within sectors and within organizations. It will also vary according to which "fair information principle" is being discussed and it will vary across time. For these reasons, it is impossible to measure in any definitive or general way the extent to which, and the respects in which, codes "work".

The Formation and Implementation of Privacy Codes in Canada

Even if it is impossible to compare and measure the *practice* of personal data protection, one can compare the *procedures* through which privacy codes are implemented. The aim of this section is to describe the actions taken in five key sectors to inform consumers of their rights and to raise the level of responsibility of employees for the data that they collect, process, and disseminate. This section covers the privacy codes developed by the Canadian Bankers Association, the life and property insurance industries (the Insurance Bureau of Canada and the Canadian Life and Health Insurance Association), Stentor, the Canadian Direct Marketing Association, and the Cable Television Standards Council. These are the principal codes of practice developed under trade association sponsorship and guidance in Canada. Each code emerges from a distinct set of privacy concerns in each industry. The comparisons of procedures have, therefore, to be understood within the different economic and technological contexts of different sectors, and as a response to the privacy issues inherent within those sectors.

I. Models of Implementation

(1) The Canadian Bankers Association Model Privacy Code

The Canadian Bankers Association (CBA) was established in 1891 to provide "information, research, advocacy, education, and operational support services to its members, the chartered banks of Canada".[29] Those banks are the six major chartered banks that are required by legislation to be members of the CBA.[30]

(a) The Privacy Issue and the CBA

The confidentiality of customer financial information has always been a key issue within the banking industry, and is obviously integral to the very business of processing vast quantities of highly sensitive financial information. In 1986, the CBA formally adopted the OECD Guidelines and submitted a model code of "Privacy Principles" consistent with the OECD model formally. However, the code was not adopted by the CBA's membership. Subsequent criticism of this model code at a meeting of the OECD prompted the CBA to convene a Privacy Task Force to produce a revised code of practice, in consultation with the federal Department of Justice, the Office of the Federal Privacy Commissioner, Consumer and Corporate Affairs Canada, and Finance Canada.

Negotiations ensued during 1989 and 1990, and a final version was approved by the CBA's Executive Council in December 1990. This version did not, however, meet with the approval of either the Privacy Commissioner or the Consumers' Association of

---

[29] Canadian Bankers Association, *Annual Review 1996* (Mission Statement).

[30] Bank of Montreal, Bank of Nova Scotia, Toronto Dominion Bank, National Bank of Canada, Canadian Imperial Bank of Commerce, and Royal Bank of Canada.

Canada, both of whom continued to seek revisions. Concern centered on the use of "opinions" or "judgements", data for loan decisions, the sharing of data within subsidiary and affiliated companies, and especially the use of financial data for target marketing and the related consumer right to "opt-in" or "opt-out". In response, the CBA members agreed that the member banks should consider these issues and develop provisions based on the CBA model guidelines.

The six major chartered banks (plus Citibank and the Hongkong Bank of Canada) responded subsequent to the approval of a communication plan by the CBA's Consumer Affairs Committee in August 1991. Each, however, chose a different strategy to communicate its adherence to the CBA code. In October 1991, the Royal Bank issued a separate privacy code based very closely on the CBA version. It supplemented this with a more widely distributed leaflet entitled "Straight Talk about Client Privacy".[31] In December 1991, Toronto Dominion followed with "The TD Commitment: Protecting your Privacy".[32] Citibank followed in January 1992 with its own "Privacy Code for Individual Customers".[33] The Bank of Nova Scotia then produced "ScotiaBank and You:

---

[31] Royal Bank of Canada, *Privacy Code for Individual Customers* and *Straight Talk about Client Privacy*, October 1991.

[32] Toronto Dominion Bank, *The TD Commitment: Protecting Your Privacy*, December 1991.

[33] Citibank, *Privacy Code for Individual Customers*, January 1992.

A Question of Privacy".[34] CIBC produced a brief leaflet in March 1992.[35] The Bank of Montreal issued "Your Privacy: How the Bank of Montreal Protects it".[36] The National Bank publicly declared its commitment a month later.[37] Finally, the Hongkong Bank of Canada responded in October 1993.[38]

(b) Mechanisms for Consumer Redress and Participation

The CBA code provides customers the following rights of access and correction: the "right to obtain confirmation from their banks as to whether their bank has personal information on them"; the "right to have access to personal information about them held by the bank, except for opinions and judgements"; the "right to challenge personal information about them in bank records"; the right to have those corrections conveyed to "third parties"; and the right to have a "record of disclosure" to third parties included in the personal file. The specific procedures for the exercise of these rights are established by the individual banks rather than mandated within the CBA code. No bank has designated a specific "Privacy Officer" or "Data Controller".

(c) Mechanisms for Internal Accountability

---

[34] Bank of Nova Scotia, *ScotiaBank and You: A Question of Privacy*, February 1992.

[35] Canadian Imperial Bank of Commerce, *Straight Answers: The CIBC Commitment to Privacy of Customer Information*, March 1992.

[36] Bank of Montreal, *Your Privacy: How the Bank of Montreal Protects it*, May 1992.

[37] National Bank of Canada, *Strictly Between You and Us: Confidentiality of Personal Information*, June 1992.

[38] Hongkong Bank of Canada, *Respecting Your Privacy*, October 1993.

There are several mechanisms designed generally to raise the level of responsibility of bank employees for the personal information they process. Most of these include promises to maintain the strict confidentiality of the information to which employees might have access in the course of their employment. Some of these undertakings are signed only at the time of first employment; others are more regularly communicated. In addition, audits are used to ensure accountability. Under the Bank Act, each bank must have two internal compliance audits each year. It is not clear, however, the extent to which personal information practices are under scrutiny in the audits, although information management in general is a matter for oversight. Audit reports must be submitted to a committee of the bank's Board of Directors.

(2) Life and Property Insurance

The response of the life and property insurance industries to the privacy issue has been largely similar to the banks. Two trade associations have responsibility here, the Canadian Life and Health Insurance Association (CLHIA) and the Insurance Bureau of Canada (IBC). The former was established in 1980, when the separate associations for life and health insurance were merged. The IBC dates from 1964. The IBC represents the property/casualty insurance industry (the insurance of goods) and the CLHIA deals with the insurance of persons. They are in many respects "sister" organizations. The mechanisms through which they have sought to advance the privacy issue are largely similar. They can therefore be considered jointly, even though there are some differences in the kinds of privacy issues with which each has to grapple.

(a) Privacy and the Canadian Insurance Industry

Like the banks, the insurance industry has always been concerned with the confidentiality of customer information. Both the CLHIA and the IBC have developed model privacy codes. The first guidelines from the CLHIA date from 1980. They were adopted by a committee of the industry, under consensus procedures. Companies were then supposed to either adhere to them or to produce their own codes that would reinforce them. Interestingly, they were also tabled in the Ontario legislature by the then Minister of Consumer and Commercial Relations, who stated that companies involved in life, accident, and sickness insurance must conform to them as a condition of doing business in Ontario. This policy was never implemented by the government, but it did serve to highlight the importance of the issue and further action by the CLHIA.

Other factors also contributed to a general desire to address the privacy issue. The development of consumer credit legislation, for instance, had certain ramifications for insurance. In addition, the mid-1980s witnessed enormous publicity over the use of information about AIDS, during which time the industry began to realize the detrimental effects the virus could have on life expectancy and began to consider the circumstances under which HIV blood tests should be used in the underwriting process. The CLHIA adopted guidelines for the fair use of HIV data in 1987.[39] Finally, the impending Quebec

---

[39] Canadian Life and Health Insurance Association, *Guidelines with Respect to AIDS, for the Sale and Underwriting of Life and Health Insurance*, November 1987.

legislation motivated the CLHIA to establish a committee to review and update the 1980 guidelines. These were adopted in March 1993.[40]

The IBC's involvement in privacy is somewhat more recent. The deregulation of the finance industry in the mid-1980s was an important motivating factor. However, the more proximate causes of the IBC's desire to develop an industry code were Bill 68 and the data protection regulations proposed by the Senate Banking Committee. A model privacy code was therefore approved in November 1992, after a process of consultation and negotiation by a representative privacy committee. The code adopts the OECD Guidelines to the issues relevant within the property and casualty industry. The code states that "member insurance companies of the IBC shall agree to adhere to the model privacy codes and individual insurers may adopt additional measures for the protection of privacy of personal information".[41] At present, the IBC's members are considering the most appropriate ways to promote the guidelines at the company level.

(b) Mechanisms for Consumer Redress and Participation

The general model for implementing the codes within the insurance industry is similar, if not identical, to that of the banks. Primary responsibility rests with the individual companies to resolve complaints as and when they arise. Under the CLHIA code, each company is supposed to: "designate an officer to receive complaints and

---

[40] CLHIA, *Right to Privacy Guidelines*, March 1993.

[41] IBC, *Model Insurance Code for the Individual Insurance Customer*, November 30, 1992.

establish procedures for receiving and resolving complaints".[42] The IBC code stipulates that "property and casualty insurance companies shall inform their customers of their privacy and complaint handling procedures".[43] Access and correction rights are provided in both codes in much the same way, consistent with the OECD framework. With certain exemptions, principally for "opinions and judgements", there are rights to know what is held, to access personally related files, and to request corrections and/or erasures.

(c) Mechanisms for Internal Accountability

Like the banks, most member companies of the CLHIA and the IBC require the regular signing of statements of compliance by employees. That of London Life, for instance, includes a fairly lengthy statement about the importance of the privacy of information in the company's relations with customers. The company's code requires that the "signatures of every employee at or above the manager level will be required annually on the Statement of Compliance form to confirm the employee's compliance with the Code of Business Conduct".[44] The principle of accountability in the IBC code is also promoted by the provision that "each insurer shall identify and make known the officer responsible for the protection of personal information".[45] These devices can provide useful ways to improve the culture of privacy within an organization.

---

[42] CLHIA, *Right to Privacy Guidelines*, March 1993, Section 8.

[43] IBC, *Model Privacy Code*, November 1992, Section 10.

[44] London Life, *Code of Business Conduct*, p. 13.

[45] IBC, *Model Privacy Code*, Section 9.

(3) The Stentor Model Privacy Code

The Stentor alliance[46] was created in the late 1980s to meet the challenges of deregulation in telecommunications. It serves as an integrated strategic alliance to manage the network, to reach collective decisions on policy questions, and to respond to threats from competition in the long-distance and local market. Policies for the member companies of the Stentor Alliance are coordinated through Stentor Telecom Policy Inc. (STPI).

(a) Privacy and Stentor

There were a number of external motivating factors which led to the publication of Stentor's "Code of Fair Information Practices" in 1992.[47] On the political level, there was the publication by Perrin Beatty, then Minister of Communications, of the telecommunications privacy principles, and the later abortive attempt to establish a Telecommunications Privacy Protection Agency (TPPA) to implement them. In addition, there was the development of legislation to protect the privacy of cellular telephone calls. The experience with the initial introduction of call management services also convinced Stentor that the assessment of privacy risk had to be built into the early stages of product and service development.[48]

---

[46] BC Tel, AGT Limited, the Manitoba Telephone System, Bell Canada, Quebec-Telephone, New Brunswick Telephone Co., Island Telephone Company, Maritime Telephone and Telegraph Co., Newfoundland telephone Co., AGT Cellular, BC Cellular, BCE Mobile Communications Inc., MT&T Mobile Inc., NorthwestTel, and Ed Tel.

[47] Stentor Telecom Policy Inc., *Model Code of Fair Information Practices*, 1993.

[48] Stentor Telecom Policy Inc., *Guidelines for Assessing the Privacy Implications* (continued...)

Finally, wider economic changes had a key influence. The advent of competition between long-distance services raised a number of issues about the collection of personal information, particularly customer lists and directory databases. The telephone companies faced a new situation in which they were monopoly suppliers for some services and competitive suppliers for others. This raised the possibility of using the privacy of customer lists as a justification for preventing competition. It also raised the need for greater security and data protection measures within the telephone companies.

(b) Mechanisms for Consumer Redress and Participation

A number of vehicles are used to inform consumers of their rights with respect to privacy. The "Terms of Service" included in the "White Pages" provide a standardized statement about the "Confidentiality of Customer Records". Some directories also provide an additional commitment to the observation of privacy rights. These outlets are supplemented by billing inserts that offer similar guidance. Finally, some companies have published separate consumer privacy guidance books.

At the present time, the practices of member companies vary considerably. Most are still in the process of deciding on the specific mechanisms through which the privacy code should be implemented, and some member companies have been more proactive than others. In addition, no separate complaints resolution process for privacy concerns has been established. The typical process in all Stentor companies is for the customer service representatives to deal with any complaints first of all. If unresolved, a complaint would

---

[48](...continued)
of New Products and Services, 1993.

then be referred to senior management. Only at Bell Canada has a "Privacy Ombudsman" been established to deal with privacy concerns at a company level.

(c) Mechanisms for Internal Accountability

The confidentiality of customer information has long been a matter of corporate policy, as reflected by earlier codes of business standards. Privacy policy more widely defined, however, has required a rethinking of training processes and, in some cases, a redrafting of operating manuals. For example, a two-phase implementation framework is currently being developed at AGT Limited of Alberta in consultation with employees, customers, and various departments within the company. Other member companies are in the throes of developing their corporate strategies for the communication and implementation of fair information principles throughout their organizations.

(4) The Canadian Direct Marketing Association

The Canadian Direct Marketing Association (CDMA) was founded in 1967. It currently represents 460 national corporate members, 300 individuals members, and 350 regional members who do business in Canada. Revenue from different forms of direct marketing was claimed to be at least $9.1 billion in 1995. Over two hundred thousand full-time jobs are dependent on the provision of direct marketing services. These include: the marketing of consumer goods and services; business-to-business and catalogue sales; solicitations for charitable donations; and broadcasting. The CDMA claims to represent companies responsible for over eighty percent of direct marketing sales in Canada.

(a) Privacy and Canadian Direct Marketing

Consumer concern about direct marketing has historically been high. A 1992 Gallup poll, for instance, found that sixty-three percent of respondents considered unsolicited telephone calls an invasion of privacy. Seventy-nine percent believed that the practice of sharing lists of potential customers required "regulation by authorities".[49] However, the CDMA's efforts to address such concerns actually began in the late 1970s. At this time, "Operation Integrity" was launched, in cooperation with the Department of Consumer and Corporate Affairs. This established a self-regulatory mechanism for the handling of consumer complaints. Later, the issue grew in significance when a mailing preference service and telephone preference service were established in the early 1980s. These services allowed consumers to reduce the overall amount of direct mail and telemarketing calls. In 1991, a Privacy Task Force was established to develop a Privacy Code for all CDMA members. This group met throughout 1992, concurrent with a lobbying effort in Quebec. A set of Draft Principles was developed in consultation with the membership and the Federal Privacy Commissioner. This was later translated into a Privacy Code that was issued, with a great deal of publicity, in January 1993. Most recently, the CDMA has called on the federal government to enact a set of privacy principles in legislation that would require each industry to develop a specific privacy code.[50]

---

[49] "Few Happy to Hear from Telemarketers," *Marketing*, August 17, 1992.

[50] This call was made by CDMA President and C.E.O., John Gustavson, in October 1995.

(b) Mechanisms for Consumer Redress and Participation

The CDMA Privacy Code has been carefully developed to address the issues that confront direct marketing; it does not simply translate the existing OECD Guidelines. Consequently, its principles are worded in less legalistic and probably more user-friendly language. Like the banking and insurance codes, however, its implementation rests chiefly on consumer actions and complaints.

Principle one of the code attempts to give "consumers control of how information about them is used". This represents the most significant change in policy. As of January 1994, all new customers must be given a "meaningful opportunity to remove their name or other information for any further marketing purposes by a third party".[51] All existing customers must have been offered the same opportunity by January 1, 1995. Furthermore, this opportunity must be provided *before* any information is transferred and it must be repeated once every three years.

The second principle provides rights of access and correction to customer files and the right to question and correct erroneous information. The consumer also has the right to "know the source of his or her name used in any direct marketing program." Marketers must make "all reasonable efforts" to help customers in this regard, bearing in mind the technical constraints in the file transfer and merging process.[52]

Principle three enables consumers to reduce the amount of mail they receive. The consumer must write to the CDMA, at which point his or her name, address, and

---

[51] CDMA, *Privacy Code*, January 1993, p. 1.

[52] CDMA, *Privacy Code: Guidelines for Implementation*, p. 2.

telephone number are then registered on a "delete file" and distributed to association members four times a year. This information is maintained in delete files for three years, after which consumers have to request further registration. Subscribers to this service may continue to receive mail from non-association members, such as local merchants, professional associations, and political candidates. There are currently 220,000 people using this service, representing 165,000 Canadian households.

(c) Mechanisms for Corporate and Employee Accountability

The last four principles of the code place obligations on the data user. Principle four states that "all those involved in the transfer, rental, sale or exchange of mailing lists must establish and agree upon the exact nature of the list's intended usage prior to permission being given to use the list or transfer the information". Normally, companies consider this proprietary information, and conditions for transfer are contractual documents between list renter and list user. It is possible that this could become standard practice across Canada. Principles of security and confidentiality (Principles five and six) may be implemented through similar contractual mechanisms, or industry-specific codes.

The code concludes by discussing enforcement and is quite specific about the mechanisms available. A four-pronged approach is outlined: (1) designated privacy managers; (2) moral suasion by members towards non-members, including "strong encouragement to choose to do business only with companies who comply with the code"; (3) publicized expulsion of members for willful violation of the code after "due process";

and (4) a consumer awareness program that encourages them to "look for the CDMA logo".[53]

Given the sensitivity of most of the direct marketing industry to privacy questions, market pressures are clearly strong. The threat of expulsion, with the attendant negative publicity, has at least on one occasion brought a recalcitrant member into line. Thus, unlike the codes of practice promulgated by the banking, insurance, and telecommunications industries, which are "models" for members to follow, the CDMA code is compulsory. Each member must sign an agreement to comply with the Code each year, upon their annual renewal in the Association. This is an important distinction as member companies may not "adapt" the CDMA principles to their own needs and still remain a member of the Association. However, there is no auditing or investigative function for the CDMA. Like other trade associations, its enforcement role is chiefly a reactive one.

(5) The Cable Television Standards Code

Standards and policy for the Canadian cable television industry are established under a model of self-regulation that is inherently different from that for banking, insurance, direct marketing, and telecommunications. This model has been described earlier as a "foundation model". It formed the basis of the recommendation that the privacy principles for the telecommunications industry as a whole should be self-regulated through the TPPA, funded through a Canadian Telecommunications Privacy Foundation. It is also similar to the model under which the Canadian Broadcasting Council receives

---

[53] CDMA, *Privacy Code: Guidelines for Implementation*, p. 4.

complaints and administers standards on broadcasting content. The operation of the foundation model in the context of the Canadian cable television industry therefore requires careful consideration.

The Canadian Cable Television Association (CCTA) began about forty years ago, and operated as a typical industry association. From 1968 cable television operations were governed by the CRTC, though it was found that CRTC decision making was unacceptably slow for an industry in which new technologies and services were developing at a rapid pace, and which was becoming increasingly competitive. A consistent set of industry standards was not likely to be forthcoming from the reactive process of CRTC review. Pressure mounted for a self-regulatory system in the 1980s.

The current decision making structure was finally established in 1988, with the encouragement and support of the CRTC, although it took three or four years for the entire process to be fully operational. Three separate entities now constitute the cable industry's self-regulatory system. The CCTA is the industry's lobbying arm and the body that develops codes, standards, and guidelines under the licencing and oversight authority of the CRTC.

Collectively, the member companies pay dues to a Cable Television Standards Foundation, a separate corporation open for membership to all licensed cable television companies. The foundation represents around ninety different cable companies, which together operate 1,279 licensed cable television systems, serving more than seven million Canadian households. The property and business of the Foundation is managed by a Board of five Directors, elected annually by the members who represent different regions

and large, small, and medium sized companies alike. A fee of 5.5c per cable subscriber is paid each year to fund the Foundation's operations. The lion's share of funding is provided by the ten largest multi-systems operations.

The principal purpose for the establishment of the Foundation is to support a three-member Cable Television Standards Council (CTSC), which administers standards, codes, and guidelines as well as mediates disputes between licensees and subscribers. This is intended to establish a clear structural separation between the functions of industry lobbying and those of administration, oversight, and complaints resolution.

Membership in the Foundation is voluntary. Once a licensee has become a member, however, compliance with industry standards is compulsory. Member companies consent to the referral of questions arising with respect to the interpretation or implementation of the CCTA's codes, standards, and guidelines to the Cable Television Standards Council and, agree to be "bound by the mandate, authority, practices, and procedures of the Council".[54] Use of the CTSC's logo symbolizes adherence to these standards.

(a) Privacy and Canadian Cable Television

The self-regulatory model was established to respond to a wide range of pressures in order to forestall governmental intervention and regulation in a number of areas. Privacy issues were perhaps a marginal consideration in this process. Nevertheless, the issue has been of concern to the cable industry from the outset, given the value and sensitivity of the information concerning viewing habits that cable operators collect. The

---

[54] Cable Television Standards Council, *Fact Sheet*, May 18, 1994.

CCTA developed some privacy principles in June 1984 in consultation with the Privacy Commissioner at that time, John Grace.[55]

The principles established by the 1984 code were later scrapped, however, when the Cable Television Standards Foundation was set up. There is now no separate and identifiable "Privacy Code". Privacy standards are incorporated into the general set of *Cable Television Customer Standards*, which cover all aspects of service and operation. Within these standards, though, is a prominent commitment to "Confidentiality and Security". In a departure from practice in other industries, the cable industry did not try to reinvent the wheel by negotiating a separate set of principles. In an innovative move that obviously saved much time and effort, they simply stated that the industry complies with the principles of the federal Privacy Act of 1982. Each member company will:

1. pursuant to the Privacy Act, maintain as confidential all personal data required by the company in order to provide services,
2. allow a customer to inspect his or her service record material on file with the cable company upon reasonable notice and during normal office hours,
3. upon request by a customer, remove his or her name from listings for mail and telephone solicitation,
4. ensure that all cable company employees provide identification, including a photograph, when requesting entrance to customers' premises.[56]

---

[55] Canadian Cable Television Association, *Cable Subscriber Privacy Policy*, June 13, 1984.

[56] Cable Television Standards Council, *Cable Television Customer Service*

(continued...)

(b) Mechanisms for Individual Redress and Participation

The implementation of privacy standards within the cable industry cannot be distinguished from the general effort to self-regulate on a range of service and operation standards. In order to redirect potential complaints from the CRTC to the CTSC, there has been a concerted effort to publicize the existence and role of the CTSC. For example, sometimes information about the complaints procedure is included in *TV Guide*. As a result, there has been a notable reduction in the number of complaints to the CRTC about cable service. The CTSC sees itself as a kind of "better business bureau" for the cable industry.

The complaints process is outlined in some detail in the *Service Standards*, and was initially approved by the CRTC. It is explicitly referred to as an "adjudication process". Complaints not initially resolved are referred to the Council. If conciliation is ineffective, a decision by the Council is rendered that is "not subject to approval or review by the cable television industry or any of its organizations".[57] The standards also allow customer access to "service record material", but they do not explicitly mention a right to correct or delete erroneous personal information. The standards allow an opt-out from the receipt of mail and telephone solicitations by writing to the company. They do not as yet provide "opt-out boxes" on billing inserts and the like, though this is currently under consideration by the CCTA's Privacy Task Force.

---

[56](...continued)
Standards, June 1991, Section II.

[57] Cable Television Standards Council, *Cable Television Customer Service Standards*, June 1991, Section VIII.

(c) Mechanisms for Corporate and Employee Responsibility

The training of staff is the sole responsibility of individual cable operators. Some, like Videotron, have training programs that include a component on privacy, though there is no complete information on the extent to which this is done across the country. Each cable operator has a designated complaints officer, but none has a specific "Privacy Officer" or "Data Controller".

Unlike the other industries discussed in this section, the foundation model does permit an auditing function. Two audits are performed annually in each region by the CTSC's Executive Director. Again, the functional separation between standards-setting and implementation inherent in the foundation model permits an investigative role that cannot be preformed by the more traditional industry association. The ultimate sanction is expulsion from the Foundation, though this has never occurred.

II. Summary of Models of Implementation

The privacy codes of practice of the five industries analysed above have a number of interesting similarities, but they also reflect three different models of implementation. Those of the CBA, the insurance industry, and Stentor are of the typical *Sectoral Model Privacy Code*. This has the following characteristics:

1. An adaptation of the OECD Guidelines in consultation with member companies and outside institutions (most notably the Office of the Privacy Commissioner of Canada).
2. Responsibility for complaints resolution rests with the individual member company.
3. Responsibility for consumer awareness rests chiefly with the individual member company.

4. Responsibility for employee training and awareness rests chiefly with the individual member company.

5. Compliance is dependent mainly on moral suasion, as well as a general but variable commitment to corporate social responsibility.

The CDMA code exhibits some slight differences. The functional, rather than sectoral, scope of the code has prompted the CDMA to play a more forceful role in its development and implementation. The CDMA code may be characterized as an *Industry Association Model*. This approach tends to have the following characteristics:

1. Policy development consists of a more radical assessment of personal information practices that produces a complete reformulation of the OECD framework.

2. Responsibility for complaints resolution rests principally with the member company, but with an explicit and formal process for complaints mediation by the association.

3. Responsibility for consumer awareness rests chiefly with the association.

4. Responsibility for employee awareness and responsibility is shared between the member company and the association.

5. Compliance is dependent on moral suasion, designated privacy managers, and threats of expulsion for non-compliance.

Finally, the policy of the cable television industry is implemented through a *Foundation Model*, of which the chief characteristics are:

1. Privacy policy is incorporated into a wider set of industry standards, the development and implementation of which take place under the oversight regime of the CRTC.

2. Responsibility for complaints resolution rests chiefly with the individual member company, but with a public mediation and adjudication role for the CTSC, funded through the Cable Television Standards Foundation.

3. Responsibility for consumer awareness rests chiefly with the CTSC.

4. Responsibility for employee awareness rests with the individual firm, but with regular auditing from the CTSC.

5. Compliance is dependent on moral suasion, a commitment to corporate social responsibility, the threat of expulsion, and the imminence of CRTC intervention.

Surveillance and Canadian Public Policy: Future Challenges

It was argued in Part I that much discussion of surveillance quickly relapses into the paranoid, where surveillance is viewed overwhelmingly and monolithically as a threat. This is especially true of those forms of analysis whose starting point is the omnipresent power of the Panopticon, but it also echoes in the idea of "Big Brother". Good reasons exist for resisting the paranoid, however. For one thing, surveillance systems emerged historically in a symbiotic relation with democratic government and the extension of citizenship rights. For another, fears about "Big Brother", concerns about democracy, and worries about personal dignity have given rise to resistance. Such resistance has been expressed in a number of ways during the past few decades of electronic surveillance expansion. In this chapter, I have examined two particular forms: legal limits on modes of data collection, storage, and use, and voluntary privacy codes of practice.

The operation of the latter, however, needs to be understood within the confusing patchwork of the former. Personal data protection policy in Canada's private sector is implemented under the following conditions: under the comprehensive data protection legislation of Bill 68 in Quebec; under sectoral provincial legislation; under partial federal regulation for some privacy-related issues; under a partial combination of provincial and federal regulation for some privacy-related issues; under potential intervention by federal oversight authorities; and under voluntary codes of practice. Thus, there is great variability in the current conditions for the protection of personal information in Canada's private sector.

The aim of this chapter has been to outline these conditions. In doing so, I have provided a context for the discussion of the background conditions and short term events that are making new policy initiatives possible at the level of the federal government. This discussion can be found in Chapter Five. In addition, I have provided a context for the discussion of mobilization movements, which tend to go beyond traditional regulatory forms of resistance to more radical opposition. This discussion can be found in Chapter Six.

I also have filled a longstanding gap in the literature on privacy and data protection. Today, privacy codes are more popular in many countries, including Canada, than they were in the past. However, there is very little on codes of practice in the literature on privacy and data protection. As such, I have described the evolution of privacy codes in Canada and presented a typology of the diverse range of instruments that have that label. In addition, I have discussed in detail the major codes of practice from the

Canadian Bankers Association, the insurance industry, Stentor, the Canadian Direct Marketing Association, and the Cable Television Standards Foundation. These codes have been compared according to the way they perform certain essential functions of consumer education, complaints resolution, employee training, and oversight.

Finally, by comparing the major codes of practice in these ways, I want to make clear that it has not been my intention to evaluate their adequacy. Data protection rules encompass an intricate blend of organizational obligations and consumer/citizen rights. There is not, then, one overall standard of workability. Instead, this chapter has commented on the overall policy picture for personal data protection in Canada. In doing so, I have contributed to the future containment of surveillance. Surveillance is a central institutional area of contemporary societies, and as such calls for forms of social analysis *and* political action that are responsible and caring. Part I of the dissertation focused on the former area; this chapter has outlined the context within which future initiatives in the latter area will develop. In the following chapter, we see that the challenge for these initiatives is to find the right balance between general standards and specific applications. That balance needs to be compatible with institutional arrangements, acceptable to business, adaptable to evolving technologies, and consistent with the legitimate privacy expectations of the general public. Let us now examine how a particular policy initiative from Industry Canada - framework legislation for the private sector - might achieve this balance.

Chapter Five: Surveillance and Future Canadian Public Policy

Reasons Behind the Proposed Privacy Legislation for the Canadian Private Sector

Part I noted that contemporary surveillance exists in an expanding range of settings, within each of which surveillance capacities are augmented and to which new technologies increasingly contribute. Far-reaching consequences follow. First, new categories of social relationships emerge, structured by the data-image. This data-image reconstitutes "selves" by piecing together bits of data drawn from diverse sources. These days, instead of surveillance being contained within discrete spheres, new technologies permit a blurring of boundaries. Computer networks transgress traditional conduits of personal information, creating myriads of new channels that defy definition. Computer matching in particular makes visible this effect, which, in conjunction with statistical analysis, isolates groups and identifies deviants with ease.

Second, surveillance carefully sifts consumers, clustering them into crude categories to be taught specific skills and educated according to their economic station. This is hardly a coercive form of surveillance, though; as noted in Part I, the evidence from marketing companies suggests that many people cheerfully comply with the consumerist order. On the other hand, such surveillance classifies together those whose market position disqualifies them from participation in the consumerist cornucopia. This same group is much more likely to experience surveillance of a carceral kind, not only from corporations, but also from welfare and policing departments. Thus, while the soft social control of surveillance may be scarcely perceptible, and for many is relatively innocuous, it also serves to perpetuate social division, particularly those on the axis of consumption.

The stock response to issues of surveillance has historically been couched in the language of privacy. Indeed, the relevant legislation in North America is normally termed "The Privacy Acts". However, it was argued in the Chapter Four that North American data protection laws tend to cover only government databanks, leaving huge swathes of commercial surveillance relatively untouched. Thus, when in 1991 Lotus advertised new business software on CD-ROM disks that revealed at the push of a button the names, addresses, marital status, and estimated income of eighty million American householders, no law stood in its way.

But soon this may be changing, at least in Canada. In September 1996 former Justice Minister Allan Rock announced that "The Government of Canada takes the position that the protection of personal information can no longer depend on whether that data is held by a public or private institution" (1996: 8). As such, Mr. Rock stated that "By the year 2000, we aim to have federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector" (1996: 7).

The depth of the federal government's commitment to these statements remains to be seen. In the meantime, though, it is important to note that Mr. Rock's comments are not new; they echo earlier statements in a report by Industry Canada issued last spring. In this report, was the conclusion that "the right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens" (Industry Canada, 1996: 25). Hence:

> As a means of encouraging business and consumer confidence in the Information Highway, the Ministers of Industry and Justice, after consultation with the

> provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

One of the aims of the dissertation is to examine the background to this announcement. To this end, Part I examined the history of surveillance and modernity. Such an examination provides a broad, long term picture against which particular and specific events in public policy can be compared. To make comparisons, though, policy analysts often find it useful to distinguish between the background conditions that make policy change possible, and the more immediate or proximate events that motivate political decisions (Simeon, 1976). As such, this chapter identifies four background conditions and three proximate events for policy reform.

There are four necessary, but not sufficient, background conditions without which Minister Manley would not have made his announcement. First, is the potential market consequences of inconsistent privacy standards within Canada, as discussed in the Introduction to the dissertation. A second and related factor is the effect of emerging data protection rules within the international arena. Third, there is evidence of strong and growing privacy concerns from the Canadian public. Finally, the fourth condition is the erosion of the boundaries between the public and private sectors as a result of shifting organizational functions in response to new technologies; this has serious implications for the effectiveness of existing public sector privacy legislation.

In addition, Minister Manley would not have made his announcement if prior work on privacy protection had not been done. This took place in three separate, but overlapping, policy arenas: (1) the Canadian Standards Association, the principal

standards-setting and certification organization in Canada; (2) the Information Highway Advisory Council, established in 1994 to advise the Department of Industry on the range of policy issues raised by the convergence of computers and telecommunications technologies; (3) and the Uniform Law Conference of Canada, an advisory body organized under the auspices of the Federal Department of Justice.

By describing the four background conditions and three proximate events listed above, I give some guidance to the future framework for privacy protection policy in Canada. That is, I suggest key features of the emerging "Canadian model" for personal data protection. Such a model is necessary insofar as it may offer some basic protections against rapid technological change and the spread of surveillance over vast tracts of social life untouched by law, such as the sphere of consumption. Finally, such a model may prompt or assist other forms of resistance to contemporary computer surveillance. These forms, which usually attempt more radical questioning and opposition to the perceived negative consequences of surveillance, are discussed in Part III.

The Background Conditions for Policy Reform

(1) The Market Implications of Inconsistent Privacy Standards

With the enactment in 1993 of Quebec's Bill 68, *An Act Respecting the Protection of Personal Information in The Private Sector*, Quebec became the only jurisdiction in North America to produce comprehensive data protection rules for the private sector. Bill 68 applies the fair information principles to all pieces of personal information collected, held, used or distributed by another person, confined mainly to enterprises engaged in an

"organized economic activity". Personal data shall be collected from and with the consent of the person concerned, and shall not be communicated, sold, leased or traded without the consent of that same person. The Access to Information Commission in Quebec (CAI), the body established under the 1982 public sector access and privacy law, is responsible for hearing complaints and rendering decisions.

Bill 68 has created three inter-related concerns for enterprises both in Quebec and in other provinces. First, Section 17 of the law states that "every person carrying on an enterprise in Quebec who communications, outside Quebec, information relating to persons residing in Quebec . . . must take reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned". This provision has yet to be enforced, but Bill 68 does give the CAI sufficient powers to prevent an outward transborder data flow if "reasonable steps" have not been taken.

Second, whether or not transborder data flow restrictions are enforced, inconsistent standards are an inconvenience for Canadian business. For businesses that operate in different provinces, the transaction costs of having to deal with different privacy laws and regulations can create uncertainty and confusion. This is a particularly acute problem for provincially regulated industries like insurance and retail. Such enterprises are obliged to grant rights to Quebec consumers that citizens in the rest of the country do not enjoy. Some businesses have thus harmonized their rules and declared that their practices in the rest of Canada conform to the Quebec standard.

Third, the patchwork can have more direct economic consequences through the unintended creation of an "unlevel playing field" that may put some businesses at a competitive disadvantage. Quebec's Bill 68 only formally covers provincially regulated entities and excludes the financial, telecommunications, and transportation sectors. At the same time, entities in those federally regulated sectors have clients and competitors (such as the insurance industry) that are covered by Bill 68 in Quebec but which are subject to few data protection rules in other provinces.

This is one reason why the extension of the federal Privacy Act to the federally regulated private sector would not produce a comprehensive set of rules for the entire marketplace. Although this option has been advocated in the past (Standing Committee on Justice and Solicitor General, 1987), it would create disadvantages for some sectors over others, and even for some businesses within sectors, such as telecommunications. Federal legislation would not extend to all possible service providers on the information highway, and would create a "patchwork privacy environment in which many market participants would be under no obligation to protect the privacy of their customers" (Stentor, 1994).

The complexity of Canada's patchwork is not only daunting to the privacy analyst, it also creates a significant and increasing set of transaction costs for businesses that operate in different jurisdictions. It is principally for these reasons that the privacy protection issue has risen to the political agenda and that the rhetoric about "marketplace rules of the road" and "level playing fields" on the information highway has overshadowed the traditional discourse about human rights and civil liberties within which privacy

protection originated. It is also the reason why the lead department in policy formulation is now Industry Canada, rather than Justice Canada.

(2) The Economic Implications of International Standards

In July 1995, the Council of Ministers and European Parliament of the European Union (EU) formally and finally adopted a "Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data". This approval was the culmination of five years of drafting and redrafting as the document passed through the complicated and lengthy EU decision making process. The aim of the *Data Protection Directive* is to "ensure a high level of protection for the privacy of individuals in all member states - and also to help ensure the free flow in information society services in the Single Market by fostering consumer confidence and minimizing differences between the Member States' rules". This reflects the underlying assumption that harmonized privacy protection legislation and the free flow of data are complementary rather than conflicting values, and that the single European market relies not only on the free flow of capital, goods and labour, but also information.

For countries such as Canada, the adoption of this directive is most important in the area of transborder personal data flows. Article 25 of the *Data Protection Directive* stipulates that "Member States shall provide that the transfer to a third party country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection". The "adequacy" of protection shall be assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations".

Particular consideration is to be given to the nature and purpose of the data and the "rules of law, both general and sectoral" and "professional rules and security measures which are complied with". This suggests that something less than a comprehensive data protection statute might be considered "adequate" and that an overall country assessment is not necessary. However, these rules and measures must be *complied with*, meaning that symbolic value statements are insufficient.

Where the Commission decides that a third country does not ensure adequate protection, member states are expected to "take the measures necessary to prevent any transfer of data of the same type to the third country in question" (Art. 25 [4]). Then the Commission "shall enter into negotiations with a view to remedying the situation" (Art. 25 [5]). It should be emphasized that if the Commission finds an inadequate level of protection, member states are *mandated*, rather than simply permitted, to prohibit the transfer through a "data embargo order". This represents a stronger approach than that embodied either within the OECD Guidelines or the Council of Europe Convention of 1981. Even though both these earlier instruments contain a principle of "equivalence" (stronger than "adequate"), neither agreement requires their signatories to block data to countries that cannot ensure an equivalent level of protection. So, whereas the *EU Data Protection Directive* adopts a weaker standard, it embodies a stronger method of enforcement.

The implementation of Article 25 poses five major problems for international businesses that rely on the transborder flows of personal data. First, commentators are generally argeed that the Europeans are not going to tolerate the existence of "data

havens" - jurisdictions in which data processing may take place because of the absence of data protection safeguards. The *EU Data Protection Directive* would be doomed to failure if multinationals could instantaneously transmit their processing offshore in order to avoid the transaction costs of having to abide by the stronger measures in force in Europe. European companies will be justifiably aggrieved if they have to abide by strong data protection rules in Europe, whilst overseas competitors can act with impunity. European citizens, and the public interest and consumer groups that represent them, will also not look kindly on the continual flouting of their privacy rights by overseas interests.

Second, the initial determination of "adequacy" will remain with the national data protection agencies who will still be implementing national laws that may diverge in some some important respects from the EU Directive. Thus, different standards for "adequacy" could still exist within the commmunity, creating confusion and unpredictability for multinationals and the need constantly to be aware of the varying regulatory systems and political interests of the different European states.

Third, there is a danger that once privacy issues enter the Commission they are likely to be influenced by wider political and economic interests. The directive does provide for the Commission to set a Europe-wide standard for acceptance of transfers to specific third countries. However, there is a danger that judgements about adequacy will be susceptible to the vagaries of the European policy process and are likely to be confused with the resolution of trade-related issues that have nothing to do with information privacy. Logrolling may therefore override the more predictable and rational pursuit of a data protection standard.

Fourth, will "adequacy" just be measured against the principles of the directive or also against the methods of enforcement and oversight? If the former, then perhaps the "voluntary" codes of practice developed by North American businesses might suffice. But perhaps the latter is a more realistic view. Adequate protection may not necessarily mean superivison by a data protection authority, but it probably means, at the very least, oversight and complaints resolution by an independent sectoral regulator.

Finally, the fifth concern with the regulation of transborder personal data flows is that neither the supervisory authority nor the data controller has the power to scrutinize the processing of personal data in another jurisdiction, nor can they be fully satisfied that data subjects can exercise their privacy rights. The directive establishes a more centralized and institutionalized process to make judgements about "adequacy". Yet these provisions will probably continue to be made on the assumption that the wordings of contracts, laws, and professional codes are reflected in practice. The directive does not get around the central dilemma inherent in the former attemtps to regulate international data transmission by the Council of Europe Convention, or through "model contracts". In the absence of an audit mechanism to ensure that personal data are processed fairly and legally in a third country, judgements about adequacy will probably continue to be made in an uncritical way, and according to the "black letter of the law" or other formal indicators.

Thus, the implementation of Article 25 has major implications for Canadian businesses, in particular for credit-granting and financial institutions, for hotel and airline reservations systems, for the direct marketing sector, and for life and property insurance (Bennett, 1997). In addition, an important implication of Article 25 is not economic but

psychological. An embarrassing aspect of the *EU Data Protection Directive* is that some countries (such as Spain and Greece) that in recent memory were governed by dictatorships now have, or will get, better privacy standards than Canada. Even some of the former Eastern European states (such as Poland, the Czech Republic, and Slovakia) have, or are in the process of passing, legislation. There are, therefore, only a handful of democratic countries that have not developed a comprehensive privacy protection policy, and Canada is one of those. As such, the impact of the *EU Data Protection Directive* has been a constant underlying theme within the recent policy debates on future privacy legislation for the Canadian private sector.

(3) Canadian Public Opinion

Empirical data about how Canadians assess specific types of personal information transactions have been sorely lacking. In 1985, however, a joint task force on privacy and computers delineated three components of privacy: privacy with regard to territory and space; privacy of the person; and privacy as a correlate of human dignity and integrity in the face of massive information collected and stored about individuals (Rankin, 1985: 325). It is on the last sense that the debate on future privacy legislation for the Canadian private sector centres.

In late 1992, a joint government and private sector survey of three thousand Canadians was conducted to explore the various dimensions of privacy (Ekos Research Associates, 1993). The results revealed that more than 90 percent of those sampled were generally concerned about privacy issues, with about one-half expressing "extreme" concern. Four out of five of the surveyed Canadians believed that computers endangered

their sense of privacy; 54 percent expressed extreme concern over the computer's ability to link personal data stored on several computers; and 60 percent believed that there is now less privacy than there was a decade ago. These concerns are not necessarily based on personal experience, given that only 18 percent of those surveyed said that they had experienced a serious privacy invasion. The report speculates that "for most Canadians concern is apparently driven by other factors such as attitudes, ethics, the experience of others, or concern about how these issues might affect them or their families in the future" (1993: p. I).

When asked to give examples of "serious invasions" of privacy, only 3 percent ventured to do so. The category that captured first place was that of crime, followed by disturbance, psychological harassment, information abuse, credit and financial data problems, and finally workplace surveillance. In commenting on these findings, the report notes that the inability to name examples of privacy abuse may be due in large measure to the invisible nature of privacy problems.

The study did find, in descending order of importance, that (a) knowledgeable people, as well as those who are least informed, tend to manifest the highest levels of concern; (b) the more transparent the rules are, the less concerned individuals are that their privacy will be violated; (c) having a sense of consent and control over the process of information storage and its release makes people feel comfortable that their privacy will not be violated; (d) those who accept the rationales given for privacy protection, and who see a benefit in it, tend to be less concerned with privacy issues; and (e) perceptions of the

legitimacy of institutions that hold information about citizens are correlated with lower levels of concern that these institutions might violate one's privacy.

Among those surveyed, women, minorities, the elderly, and the poor appeared to the most concerned about privacy. Compared with Anglophone Canadians, Francophones, who enjoy privacy protection legislation in Quebec, were more concerned about privacy violation and tended to know more about it. A slightly larger proportion of Francophones, compared with Anglophones, knew where to turn in addressing their privacy grievances (22 percent versus 17 percent).

In descending order of frequency, Canadians defined privacy to mean (a) not being watched or listened to (75 percent), (b) being in control of who has access to information (70 percent), (c) controlling what information is collected (63 percent), (d) not being disturbed at home by marketers (42 percent), and (e) not being monitored at work (36 percent).

For Canadians, government legislation was ranked as the main source of privacy protection (72 percent), followed by the application of privacy rules governing both government and business (71 percent). Some 60 percent believed that it is up to business and government to work jointly to come up with necessary guidelines, and 45 percent believed that private citizens are to be entrusted most with protecting themselves against privacy violations. Finally, one-quarter of those sampled said that they would put their trust in the business community to protect them.

A more recent survey sponsored by the Public Interest Advocacy Centre (PIAC, 1995) reveals that Canadians are particularly concerned about personal information swaps

between organizations. Seventy percent (70%) of those surveyed said they would be at least moderately concerned about such information sharing between government bodies; and the greater the individual's dependence on government bureaucracies, the greater the respondents' concerns. This was especially true for women, the less educated, and respondents from lower income households. When it comes to information sharing among private firms, the level of concern soared to 90 percent in the case of information sharing between government and private firms. The survey notes that higher income households were particularly concerned about information exchanges among private firms, perhaps because they are more likely to be targeted by marketers or charity fund raisers.

Throughout the survey results, the issue of control emerged as central. In 1992, Ekos tested the statement "I don't mind companies using information about me as long as I know about it and can stop it". The same statement was met with stronger agreement in the PIAC survey - 79 percent compared to 71 percent - with strong agreement increasing from 62 percent to 67 percent. Canadians clearly demand knowledge about and control over the uses to which their personal information might be put. Ninety-five percent (95%) of Canadians sampled wanted to be informed about collection processes and about how their personal information may be used.

Finally, the PIAC survey also found that 73 percent of respondents were unaware of any law or government program to protect their personal information, and only 17 percent of those sampled could actually cite an example. Only 14 percent of respondents knew of private business initiatives protecting personal information and fewer than one in twenty could actually cite an example. Thus, despite rising levels of concern over privacy,

Canadians display low levels of awareness about where they can go to seek recourse when their personal information is abused.

(4) The Shifting Line between the "Public" and "Private"

Finally, and of particular concern to Canada's small network of privacy and information commissioners, has been the gradual erosion of the boundaries between the "public" and the "private" sectors. This distinction is being eroded as the networking of postindustrial society cuts across organizational and functional categories within and between both public and private sectors. Spiros Simitis is a perceptive and prescient commentator on this matter: "The boundaries between the public and private sectors are blurred. Personal data, once stored, tend to become a flexible, common base of information" (1996). Commissioners thus worry "private" organizations performing "public" functions are able to circumvent protections offered by legislation like the federal Privacy Act.

For example, the current reality is that most private organizations, unlike their public counterparts, face no legal obligation to collect only relevant information, nor to disseminate that information only to those organizations that have a legitimate need to know. In addition, few private organizations are obliged to ask citizens' consent before disclosing information to third parties and few are mandated to grant citizens rights to access and correct their own files. Finally, few are mandated to maintain appropriate security safeguards.

This is particularly problematic in situations where "private" organizations require the use of personal data held in "public" agencies. Illustrations include: the use of smart

cards and automatic teller machines for the dispensing of government benefits; the matching of data on welfare recipients with bank or financial records to ascertain eligibility; the trading of government personal information to enhance revenue; the use of profiling techniques developed by the direct marketing industry to target segments of the population; and the use of credit reports for security checks.

In the future, the pervasiveness and flexibility of new technologies will only make it increasingly difficult to determine which organizations in which places legitimately "hold" personal data. The decentralization, flexibility, and interactivity of the "information highway" is also a constant theme, which leads to calls from the Federal Privacy Commissioner, among others, for some clear and common "rules of the road".

The Proximate Causes of Policy Reform

(1) The Canadian Standards Association's Model Code for the Protection of Personal Information

Any discussion of recent developments in Canadian privacy protection should properly begin with the initiative that has attracted the most international attention to date, the successful negotiation of a certifiable standard for personal data protection (Q830) through the Canadian Standards Association (CSA). Since 1992, a committee representing government, business, and consumer interests has been negotiating a Model Code for the Protection of Personal Information. The starting point was the 1981 OECD Guidelines (OECD, 1981), revised and adapted to the Canadian context with reference to the Quebec legislation, and the EU Directive. This was approved without dissent in

September 1995, subsequently approved by the Standards Council of Canada, and published as a "National Standard of Canada" in March 1996.

Brokered among the major stakeholders, the code is designed to add some uniformity to data protection policy and practice within the Canadian private sector. It represents a very important consensus, and it has doubtless been a valuable opportunity for participants in the process to think about the problems of privacy protection and to grapple with these complex issues from scratch.

The CSA Code is based upon ten interrelated principles:

1. Accountability. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent. The knowledge and consent of the individual are required for the use or disclosure of personal information, except where appropriate.

4. Limiting Collection. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting use, disclosure, and retention. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy. Personal information shall be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance. An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

To each is attached a commentary, designed to explain how each principle should be interpreted and applied. The CSA Code is also accompanied by a workbook, which provides in greater detail practical advice about how organizations might implement the principles (CSA, 1996).

It is crucial to appreciate the distinction between this instrument and the traditional company or sectoral "codes of practice" discussed in Chapter Four. Unlike codes of practice, the CSA Code is a *standard* that might be subjected to the same kind of certification and registration procedures used for other standards, despite the fact that it is

not the kind of "hard" standard typically used within the manufacturing industry. Nevertheless, it does have certain parallels to the range of "quality management standards" within the ISO 9000 series that have been rapidly permeating the Canadian and American private sectors, as well as with the environmental standards in the ISO 14000 series. Thus, in the same way that a company might be forced to register to ISO 9000 in order to convince its customers that it has adopted a level of "quality management", a similar system of accreditation could be developed to the privacy standard, where effective data protection is demanded within the Canadian or international marketplace. The price of maintaining a registration to the standard would be the development and implementation of an appropriate privacy policy and subscription to independent and regular privacy audits.

Of course, not all businesses would be expected to go to the kind of trouble and expense of registering to ISO 9000. The registration scheme for privacy would also require procedures applicable to the smaller business. The scheme requires an appropriate balance between the encouragement of registration on the one hand, and the prevention of symbolic claims about policies and practices on the other. It also requires an appropriate publicity vehicle, so that any consumer can find out who has registered to the standard and who has not. A "Privacy Good Book" in the form of a Privacy Register would have to accompany the registration scheme (Bennett, 1995).

The standard might spread through a number of different incentives: by moral suasion; by the desire to avoid adverse publicity; by the desire to gain a competitive advantage; by reference to the standard in private contracts; by registration to the privacy

standard in conjunction with registration to ISO 9000; by reference to the standard when government "contracts out" data processing services; by pressure from research funding agencies; by the regulation of inter-provincial data flows in Quebec's Bill 68; and by the use of the "adequacy" provisions in the EU Directive by European data protection authorities. Canadian and foreign regulatory bodies can even now insist that the receipt of personal data within Canada be accompanied by registration to the CSA Code.

As outlined, registration to the CSA Code would provide a more consistent yardstick by which to observe and evaluate company personal information practices. However, the major value of the Code is that it has been openly negotiated by industry, consumer representatives, and government. It represents a national consensus on the standards for privacy protection expressed within the ten clearly articulated principles listed above. The substance of a privacy protection policy has thus been brokered.[58] The CSA negotiation constitutes a crucial stage in the development of a national public policy. Any federal legislation will undoubtedly be based upon this standard.

(2) The Information Highway Advisory Council

Like many governments elsewhere, the Canadian federal government decided in 1994 to establish a high-profile commission to examine all aspects of the Canadian "information highway", including issues of privacy and security. In its 1995 report, the

---

[58] In September 1996, the Quality Management Institute (QMI) of the CSA announced its "Recognition Program" based on a three-tier process of declaration, certification, and registration, each with progressively more onerous and regular auditing requirements.

Information Highway Advisory Council (IHAC), which comprised a majority of business representatives, advised the federal government to:

> create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA Model Code, while allowing the flexibility to determine how they will refine their own codes.

The report goes on to recommend that the federal government, "in cooperation with the CSA Working Group on Privacy and other interested parties, study the development of effective oversight and enforcement mechanisms"(IHAC, 1995: 141).

In May 1996, federal Industry Minister John Manley released the government's response to the IHAC report, in which it was concluded that "the right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens" (Industry Canada, 1996: 25). Hence:

> As a means of encouraging business and consumer confidence in the Information Highway, the Ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

This option immediately raises the question of whether indeed the federal government has the constitutional authority to legislate in this area. Legal opinions differ, although it is by no means certain that the provinces would regard such legislation as an undue encroachment into provincial jurisdiction. However, credible constitutional arguments can be advanced that as the "information highway" spans provincial borders, an

appropriate and common set of rules is in the interests of "trade and commerce" or of "peace, order and good government" (Lawson, 1995).

The significance of IHAC's recommendation lies in the broad support from the *private* sector participants on the council, even though most industrial associations were still publicly supporting self-regulation (Akay, 1995). Subsequently, however, the Canadian Direct Marketing Association became the first industrial group to endorse a legislative approach in its October 1995 call for national legislation based on the CSA standard (CDMA, 1995). It probably did so because it was confident that its members could abide by the CSA standard, and because direct marketers who were non-members would then be forced to play by the same rules. In doing so, the CDMA broke ranks with other private sector associations. This move could prove to be profoundly important. Any business interest that wishes to oppose privacy legislation for the Canadian private sector must not only argue against Privacy Commissioners and advocates, it must also now oppose the CDMA.

(3) The Uniform Law Conference of Canada

Canada is one of the most decentralized federations in the world. Few policy areas are solely the responsibility of the federal government and privacy protection is no exception. Any constitutional justification for a federal responsibility in this area immediately confronts a division of powers that grants "property and civil rights" to the provincial governments. Moreover, constitutionally, the federal government is only responsible for regulating the financial, telecommunications, and transportation sectors. All else, including retail, consumer credit, insurance, and so on, is strictly under provincial

competence. Therefore, any legislative approach to data protection not based on a uniform policy would only exacerbate the "patchwork" problem, and may even create marketplace distortions and "un-level playing fields" (Bennett, 1996).

In light of this, the Uniform Law Conference of Canada (ULCC) was called on in 1995 by the Information Highway Advisory Council. It was felt that the ULCC could play a vital role in the development of data protection legislation by ensuring a consistency between federal and provincial approaches. As such, a task force was created to come up with recommendations for a "Uniform Personal Information Protection Act". This consultation took place with private sector, consumer, and government representatives as well as with data protection experts throughout 1996. A draft Act was released to members of the task force in March 1997.

The draft Act, known as the *Private Sector Protection of Personal Information Act*, is most closely based on Quebec's Bill 68, the first privacy Act in North America to extend to the private sector. As written, the Act applies to the federal government, but its concepts are meant to be applicable in all jurisdictions. The three aspects of the Act that are the most noteworthy are: (1) the deviations from the Canadian Standards Association's (CSA) principles; (2) the oversight powers of the Privacy Commission; and (3) the balance drawn between personal information protection and legitimate information use by organizations.

(a) Deviations from the CSA Principles

Sections of the draft Act parallel most of the provisions of the CSA Code. There are deviations, however, ranging from the Act's more detailed listing of personal

information to include fingerprints and blood type (although, curiously, no mention of DNA or blood testing); to a specific "carving out" for personal information used by the media; and a requirement that policies and practices relating to security measures be conveyed to the public. This last point extends beyond the requirement of the CSA Code that information "be protected by security safeguards appropriate to the sensitivity of the information". Ironically, providing the public with details on security policies and practices can actually diminish security effectiveness (Peladeau, 1996).

In addition, personal information may be used for study, research or statistical purposes upon approval by the Privacy Commission. This provision may go a long way toward resolving concerns from the medical community about access to personal data, but raises corresponding questions about the Commission's discretionary powers. There is no opportunity built into the Act for individuals to challenge Commission decisions in this area.

Finally, the Act also requires that all requests to have access or corrections made to files must be in writing. It further stipulates a precise time frame of thirty days in which organizations must respond to such requests, with failure to respond within the specified period being deemed under the Act a refusal to respond. The CSA Code does not impose any such requirements, although it calls for response within a "reasonable time frame".

These examples of deviations from the CSA Code are significant because they illustrate a point that was made by one member of the ULCC working group who suggested that "legislation should not impose stricter obligations than those found in the

CSA Code, thus leaving room for organizations to voluntarily choose areas which they may wish to enhance, depending on their business" (Long, 1997).

(b) Powers of the Privacy Commission

To trigger action on the part of the Commission, a written request must be submitted, either by an individual or a group of individuals with a complaint or unresolvable disagreement within an organization. Under the draft Act, the Commission has "all the powers necessary for the exercise of its jurisdiction and may make any order it considers appropriate . . . and may rule on any issue of fact or law". The Act specifies that a decision on a question of fact is final and may *not* be appealed, while decisions based on a question of law or jurisdiction may be appealed. This parallels the approach in most judicial proceedings - that the facts, once established, are immutable. However, many of the cases to be dealt with by the Commission will likely revolve around differing interpretations of facts. For example, in the case of organizations providing information to third parties with consent, an agreed-upon interpretation of a phrase such as "related organization" may be difficult to arrive at. Thus, any interpretation unilaterally determined to be a "fact" by the Commission should also probably be subject to appeal.

(c) The Information-Use Balance

Finally, the *Private Sector Protection of Personal Information Act* was drafted by a committee representing business, government, and consumers who argued that the privacy problem is essentially one of establishing an appropriate balance between the demands of individuals for personal autonomy and the demands of organizations for information about them. However, in the draft Act there are a number of sections that

overtly tip the balance in favour of individuals. For example, the Act specifies that "where there is a question of whether the personal information is necessary or not, the information will be deemed not necessary". Who does the "deeming" in this case and on what basis is unclear. In contrast, the CSA Code calls for organizations to clearly define and explain information gathering requirements, which must be clearly linked to a purpose. The individual can then challenge the purpose. Thus, the collection of certain information is never deemed unnecessary *before* a challenge and subsequent review process have taken place. Under the proposed Act, there are no such safeguards for organizations who often argue that individual demands for "personalized" products and services push them into collecting more and more personal data.

The Elements of a Canadian Data Protection Policy for the Private Sector

By tracing the four background conditions and three proximate events described above, I am able to conclude that a distinctively Canadian privacy protection policy is taking shape. The essential nature of this policy has the following features.

(a) Legislation to the Standard

It is probable that any federal and/or provincial legislation will be based on the CSA Code. Former Justice Minister Allan Rock described this agreement as a "milestone" on the road to legislation for the year 2000 because it provides a national "consensus document". Even before national legislation is drafted, the CSA standard can be referenced in law, as have been approximately one-third of CSA's published standards. Most of these standards relate to minimum technical specifications for products procured

by government. Increasingly, however, performance standards, such as those for quality management or environmental protection, are being used in order to implement statute, regulation and court order. There is nothing to stop federal and/or provincial authorities from using Q830 in a similar way.

The federal government, however, envisages a more comprehensive "framework" or "shell" legislation at the federal level; a general statement of principles and obligations, leaving the functions of complaints resolution, investigation, auditing, and so on as a matter for further analysis. Individual business sectors would still have the freedom to develop their own specific codes of practice in conformity with the general standard. Thus, as Ian Lawson points out, the "higher purpose of the Model Code is for it to be adopted-by-reference as a legislative standard to which the private sector must comply as a condition of using personal information on the information highway" (1995: 43).

Registration to the CSA Code contributes a crucial mechanism for enforcement within any potential regulatory system. Registration to the privacy standard can complement almost any current or future, contractual or regulatory, provincial or federal, sectoral or comprehensive provisions for personal data protection. It can be used to reward good practice and to bring the recalcitrants into line. It is also becoming apparent that standards certification is entirely consistent with the personal data practices on the Internet. For instance, recent pilot projects, such as that of the Center for Democracy and Technology (www.cdt.org), have tried to classify Web pages according to their "privacy friendliness".

Finally, some have also suggested that regulators be given the power to order registration to the standard. Thus, if a pattern of complaints arose about a particular business, privacy commissioners or the courts could require registration to the standard, triggering the code development and audit process and passing the costs to the data user. A process of registration to the standard adds a compliance instrument that is not present within any other data protection regime. The potential to require (by law or regulation) a registration to the standard can relieve privacy commissioners of expensive and time consuming compliance monitoring functions. Registration to the standard is also potentially a more effective sanction than a fine. The loss of the CSA "mark" can have real consequences for business. I quote Jason Meyers, chief economist at the Canadian Manufacturers Association: "The prospect of a $50,000 government fine for breaching the law pales in comparison to losing your entire customer base because the firm fails to meet its ISO-9000 requirements" (McInnes, 1996: 34).

(b) The Privacy "Toolkit" Approach

There are a range of tools within the repertoire of possible policy instruments. Four are outlined within Industry Canada's publication *Privacy and the Canadian Information Highway* (1994): legislation and regulation; voluntary codes and standards; technological solutions; and consumer education. The recognition of the complementarity of these privacy solutions is perhaps stronger in Canada than in most other societies. Former Justice Minister Allan Rock speaks about policy development taking place along four tracks (Rock, 1996):

> One track runs through the legislatures of the land. In this case, the task includes the updating of existing statutes and the writing of new ones that respond to the needs of the time. Another track runs through the research and development labs of the information technology industry . . . New information technology not only generates new pressures on effective privacy rights, but new methods for containing them . . . The third track runs through every business enterprise and private sector institution in Canada. Total privacy protection will never be achieved simply by legislation. To be effective, the system must engage the wholehearted support and cooperation of the private sector in general . . . The fourth track runs right down Main Street. In any system designed to protect human rights - and privacy is exactly that - an informed public is an essential component.

Each of these four "tracks" contributes to a "mosaic of solutions" (Cavoukian and Tapscott, 1995). Recognition for this mosaic is explained by the coincidental arrival of private sector privacy protection policy on the federal agenda with the advent of innovative technical solutions. For example, the development of new privacy enhancing technologies in the past ten years has allowed federal policy makers to consider these solutions on a par with more traditional regulatory and self-regulatory approaches (Ontario Information and Privacy Commissioner, 1995).

(c) A Central Role for Self-Regulation

Colin Bennett has argued that "almost by default, Canada has become the only country in the advanced industrialized world that has begun seriously the process of promoting privacy protection from the bottom up" (1995: 119-20). For example, there are probably more privacy codes in Canada than in any other society, especially from sectoral trade associations (e.g., CTSC, 1991; Stentor, 1992; CDMA, 1993; CLHIA, 1993; and CBA, 1996). Codes of practice are, and will continue to be, a feature of privacy protection policy in Canada.

There is, however, a key distinction between voluntarism and self-regulation. The former implies that public policy should remain indifferent to the policies and practices pursued. It implies that government should simply trust business to pursue privacy friendly practices but has no interest in setting an overall standard. This has been the position of the Canadian and American federal governments to date. A self-regulatory regime, on the other hand, establishes in law the standard and grants business the authority to regulate its own practices. The key difference is that a legislated standard is set, and that both individual and organization know that when self-regulation breaks down, the policy instruments established under the law can intervene.

Intervention, however, can be a lengthy and complicated matter. For instance, if codes are not formally endorsed by a data protection authority, then they may contain language that conflicts with the wording of the law, and confusion about applicability and enforcement may ensue. On the other hand, if a more formal ratification process is laid out (as in New Zealand and the Netherlands), this can lead to the bureaucratization of a process that, in theory, is supposed to allow for the flexibility of self-regulation. Thus, Canadian policy makers may have difficulty in determining the role that codes of practice should play in a data protection regime. In this regard, overseas experience suggests that codes of practice that enjoy any form of legal status can be difficult and time-consuming to negotiate (Bennett, 1996).

(d) "Light" Oversight and Enforcement

Canada will undoubtedly avoid the bureaucratic licensing and registration schemes that have been established in some European states. As such, the central oversight

agencies will probably continue to be the federal and provincial information and privacy commissioners, as these offices have established an independence, credibility and expertise in data protection. In addition, they are uniquely located within the regulatory landscape to oversee private sector legislation and resolve issues that span the public-private divide. However, these agencies only exist at the moment in Ottawa, Quebec, British Columbia, Ontario, and Alberta. The allocation of oversight responsibilities in the other provinces will need some very careful consideration in light of the constitutional division of powers and widespread policies of fiscal restraint.

Beyond Proposed Privacy Legislation for the Canadian Private Sector

This chapter has argued that slow and incremental progress is being made in Canada towards a data protection policy that displays some distinctive and perhaps innovative qualities. This approach emphasizes the use of all instruments within the "toolkit" of privacy protection. It recognizes that voluntary action from the "bottom up" is just as necessary as regulatory action from the "top down". And it comprises an innovative combination of the traditional ombudsman approach with the use of new privacy enhancing technologies and with instruments from the world of standards-setting and certification. If our federal and provincial institutions can strike the appropriate balances, Canada just might end up with a data protection policy that is not only "adequate" to meet European expectations, but far *more sensitive* than European approaches to the myriad privacy issues raised by the distributed and networked computing environment of the "information highway".

That having been said, the late twentieth century is witness to widespread, massive, unprecedented change. Economic restructuring, based on new technologies and global operations, political realignments following the end of the Cold War and the reassertion of nationalisms, and social-cultural shifts relating to consumerism, mass media, and ethnic, gender, income, and status conflicts have produced a world quite different from that of the mid-century.

A main feature of this restructuring is the ability of new information technology to handle, through the use of powerful computers, unprecedented amounts of information by both public and private organizations. Surveillance, in the broad sense of the collection and processing of personal data, is a significant aspect of this. As such, it is a central argument of the dissertation that if surveillance is to be channelled into ethically and politically appropriate directions, contemporary debates about surveillance and privacy must be explored from a variety of angles. To this end, Part I of the dissertation focused on the social and historical analysis of surveillance, concluding with the argument that constructively critical theory based on notions of *participation*, *personhood*, and *purposes* would not only go a long way in relieving us of the pessimism and paranoia bequeathed to us by the dominant Orwellian and Foucauldian models, but would also create space for genuine alternatives. Thus, I have suggested that if we are to transform our present situations into something different and desirable, the first agency would be responsible social analysis.

Responsible social analysis helps us to better understand the relation between consumption, social order, and surveillance, thereby removing common obstacles to

appropriate legal and political action. Such actions are the respective subjects of Parts II and III of the dissertation. In Part II, I outlined the current conditions for the protection of personal information in Canada's private sector, focusing in particular on legal limits on modes of data collection, storage, and use, and on voluntary privacy codes of practice. Part II concluded with a detailed description of the key features of the emerging "Canadian model" for personal data protection in the private sector, and with an analysis of how four background conditions and three proximate events have made the development of such a model possible. By describing these conditions and events, I have answered the first of two questions outlined in the dissertation: why is privacy legislation for the private sector in Canada "an idea whose time has come"?

Finally, continuing the argument that we need to be concerned with both the social analysis of surveillance *and* with its practical, legal, and organizational consequences, Part III discusses mobilization responses to surveillance and their larger relation to social movements. By analysing mobilization responses, I answer the second and final question posed in the dissertation: how can public awareness about surveillance be increased? This question is of the utmost importance because the range of surveillance capacities has increased dramatically in contemporary advanced societies, and surveillance capacities have expanded in each dimension. New categories of social relationships are now emerging in relation to the data image, and social divisions, especially those articulated with consumption, are being reinforced. If we are to respond to the current situation, then we must ask what challenges have been posed to surveillance itself. What sorts of resistance have been placed in the path of the machine, for what reasons, and with what

effects? For answers to these questions, I turn now to the third and final part of the dissertation, which examines the status and achievements of various "counter-surveillance" groups.

PART III

Chapter Six: Counter-Surveillance Responses

The Challenges to Surveillance: Technical and Mobilization Responses

It was argued in Part I that much surveillance theory is dystopian. For example, stark contrasts, helpless fear, and doom-ladden predictions are depicted in *Nineteen Eighty-Four* and the Panopticon via chosen concepts - surveillance capacities, for instance - or conscious allusions such as those to Big Brother, watching. However, I have also tried to show in Part I how the unmitigated negativism of the dystopian misleads. For instance, I have demonstrated that surveillance systems emerged historically in a symbiotic relation with democratic government and with the extension of citizenship rights. Additionally, though, I argue throughout the dissertation that surveillance never appears as an unambiguous or unmitigated evil. Rather, a more or less obvious social benefit accompanies its spread in virtually very case. Thus, surveillance does seem invariably to exhibit two faces. Under these circumstances, it is difficult to insist that surveillance is necessarily or inevitably negative in its consequences for human social life.

Nevertheless, a question raised persistently within the dissertation is, how far does new technology make a difference? Are novel features appearing on the surveillance landscape that might alter the perception of change from challenge to threat? If we review the various factors analysed earlier, we are reminded that electronic technologies facilitate the expansion of indirect, impersonal control, of more knowledgeable organizations on which modern populations are increasingly dependent. Electronic technologies have thus augmented and amplified surveillance capacities in several significant ways, so that whatever else is said about it, surveillance is clearly intensified in contemporary advanced

societies. In what ways does the quality or magnitude of this intensification present new challenges for human personhood or democratic polity today?

Two kinds of answers to this question may be offered. We may consider the actual responses to intensified surveillance that have emerged over the past few decades or so. These in turn may be divided into technical responses, those that seek legal or technological means of restricting or adding security features to surveillance systems. Examples of such responses would include technological fixes such as encryption or enhanced security, and legal remedies such as privacy or data protection law. This type of response, as well as its background conditions and proximate events, was discussed in Part II of the dissertation. The other type of response to surveillance lies in the form of mobilization movements, which seek to organize opinion or opposition to surveillance. Examples would be the activities of civil rights or consumer groups that attempt by legal, lobbying or other means to protest or limit the spread of surveillance. This type of response, which has a larger connection to social movements, is discussed in this chapter.

In this regard, I suggest that an understanding of the dynamics of social institutions in the modern world - capitalism, industrialism, the nation-state, and militarism - has led some theorists to expect to see social movements generated in opposition to those institutions. Indeed, over the past two decades theorists have argued strongly that the more conventional politics of modern societies is being challenged by social movements, whose concerns transcend traditional debates resting on class, nation, and so on (Melucci, 1989). But while the opposition of Green movements to industrialism or peace movements to militarism may appear to echo the more venerable and historically longer

term labour movements' resistance to capitalism, it is far from clear that surveillance has generated much by way of systematic opposition in terms of identifiable social movements, though there are signs that this may be changing. This chapter examines the status and achievements of such groups and movements, and also suggests possible reasons for their relative absence or weakness.

Theorizing Mobilization Responses to Surveillance

In 1987, when the Australian government proposed to establish a national electronic identity card scheme, a number of groups and individuals, encouraged by public opinion, successfully blocked the plan (Lyon, 1991). Computer scientists attacked the idea in its technical detail (Clarke, 1987), and the New South Wales Privacy Committee questioned its efficacy in reducing tax and welfare fraud (Graham, 1987). The matter was debated fiercely in the national newspapers and eventually quashed in parliament when civil libertarian Ewart Smith showed Senator John Stone a legal loophole which gave the opposition its chance to prevent the bill from becoming law.

This might be called a "mobilization response" to the challenge of surveillance, and it links the rise of surveillance society to the growth of social movements. Another perhaps more telling example would be what Langdon Winner calls the "computer populism" that rose in protest against the "Household Marketplace" software advertised by Lotus in 1993 (Winner, 1993). In this case, the organizations known as the Electronic Privacy Information Center (EPIC) and Computer Professionals for Social Responsibility (CPSR) galvanized action through national and international networking. These groups

were concerned about the lack of protection for personal identities offered by this marketing tool and about the fact that Social Security numbers were being used as universal identifiers. Although Equifax - the credit union that supplied the data to Lotus - assured the public that their product had been "misunderstood", it seems that in fact it was understood all too well.

One approach to the emergence of so-called "new social movements" is to connect them to the institutional dimensions of modernity, after the style of Giddens, for example. This would stimulate a search for identifiable organizations and groups whose activities run counter to central institutions of modernity. However, while this provides a useful springboard, it also raises several difficulties. One such is the problem of identifying the institutional spheres - where, for instance, does patriarchy feature in this scheme? Contemporary feminism clearly finds expression in "movements" today.

Another difficulty we encounter directly in relation to our theme is that while someone like Giddens writes illuminatingly on surveillance, the only movements he offers in relation to it are the rather vaguely defined "free speech", "democratic", and "human rights" movements (1985: 314 and 1991: 207). However, this apparently disappointing vagueness may turn out to be a virtue. Perhaps we should not expect there to be social movements of similar kinds, generated by specific institutional dimensions of modernity.

Now, in saying this I do not wish to imply that social movements have somehow been ironed out, flattened by the pressure of dominant political and cultural forces. Far from it. Indeed, as Alain Touraine notes, it is precisely this kind of dismissal of social movements that one hears from the disciples of Foucault (1989: 763). Granted, I have

tried to indicate how the mechanisms of social and political control are being reinforced steadily by electronic technologies. But such a conclusion manifestly does not exclude the possibility of countervailing forces gaining a significant voice (Bauman, 1988: 95). Indeed, the theorem of the dialectic of control would lead one to expect just such possibilities to emerge.

Another way to analyse social movements is through the work of Alberto Melucci (1989), who concerns himself with the need to rethink fundamentally the conventional social science interpretation of social movements. Melucci not only rejects the early nineteenth-century metaphysical image of social movements as heroes or villains acting out a script on the stage of human history. He also questions the assumptions of those twentieth-century approaches, influenced by Marxism, the Freudian tradition and theories of deprivation, which emphasize either the objective causes of collective action - the structural contradictions and crises of the social system - or its subjective dimensions, that is, the psychological motivations and preferences of individuals which lead them to band together as a social movement. Melucci argues that each of these nineteenth- and twentieth-century perspectives was founded upon the questionable assumptions that movements are a *personage*, and that collective action is a unified empirical entity whose deeper significance can be unravelled by its observers.

Traditional assumptions of this kind continue to grip present day discussions about social movements. Many observers are still inclined to speak about movements as if they had a personality of their own, while considerations of their origins continue to emphasize either the institutional processes and "interests" generated by "the system" or the

psychological preferences of their participants. Melucci argues that these traditional assumptions are no longer plausible, in part because the conflicts, actors, and forms of action in complex societies have become highly mobile and differentiated.

Additionally, though, Melucci argues that social movements must be considered as fragile and heterogeneous *social constructions*. According to Melucci, collective action is always "built" by social actors, and thus what needs to be explained in concrete terms is how movements form, that is, how they manage to mobilize individuals and groups within the framework of possibilities and constraints presented to them by the institutions of our complex societies. For Melucci, collective action must be understood in terms of the processes through which individuals communicate, negotiate, produce meanings, and make decisions within a particular social field or environment. Collective actors never act in a void. They establish relations with other actors within an already structured context, and through these interactions they produce meanings, express their needs, and constantly transform their relationships. By means of these multiple and diverse processes - which are well illustrated by Melucci's own empirical research on movement networks in the Milan area - actors construct what Melucci calls a collective identity: a movable definition of themselves and their social world, a more or less shared and dynamic understanding of the goals of their action as well as the social field of possibilities and limits within which their actions take place.

Melucci's emphasis upon the self-production of social movements is perceptive and important, and it provides a framework for understanding why, during the past few decades, new forms of action have emerged in areas previously untouched by social

conflicts. According to Melucci, conflicts develop in those areas of complex systems where there is greatest pressure on citizens to conform to institutions which produce and circulate information and symbolic codes. Complex societies, in contrast to their late nineteenth-century industrial capitalist predecessors, are systems in which the production of material goods depends increasingly upon the production of signs and social relations. The factory and the state executive are no longer the exclusive *loci* of power. Relations of power become more heterogeneous and less "naked". They become "saturated" with deliberately produced symbolic codes. And society's capacity to organize life and to produce meanings for its members expands from the factory and government office to those areas which formerly escaped controls from above. Emotional relationships, sexuality, health, and even birth and death are subjected to new forms of administrative regulation. These trends, Melucci argues, stimulate the growth of social movements, and they help explain why complex societies are not "iron cages of unfreedom" (Weber), and also why contemporary conflicts concentrate more and more on questions concerning individual identity, democracy, and the relationship between society and its natural environment.

These themes evidently bear upon recent theoretical debates concerning what is "new" about present day social movements. Do present day movements signal the permanent decline of the workers' movement? Are they indicators of major transformations of power in countries such as Canada, the United States, Britain, and Germany? Are today's movements actually new and, if so, in what sense? While Melucci is uncomfortable with the term "new social movements", he parts company with most

other contemporary commentators by specifying at least four unique features of today's movements.

First, unlike their nineteenth-century counterparts, contemporary social movements are not preoccupied with struggles over the production and distribution of material goods and resources. They challenge the administrative logic of complex systems primarily on symbolic grounds. Today's movements are more concerned with the ways in which complex societies generate information and communicate meanings to their members. This emphasis on the central role of information extends from demands for the right of citizens' access to "factual information", such as missile testing plans and the extent of the ecological damage caused by industrial spills, to debates over symbolic resources, such as the challenge of the women's movement to sexist advertising.

Second, the constituent organizations of today's movements consider themselves more than instrumental for attaining political and social goals. Actors' participation within movements is no longer a means to an end. Drawing upon Marshall McLuhan, Melucci argues that the very forms of the movements - their patterns of interpersonal relationships and decision making mechanisms - operate as a "sign" or "message" for the rest of society. The organizations of the women's movement, for instance, not only raise important questions about equality and rights. They also, at the same time, deliberately signal to the rest of society the importance of recognizing differences within complex societies. Participation within movements is considered a goal in itself because, paradoxically, actors self-consciously practise in the present the future social changes they seek. They are no longer driven by an all-embracing vision of some future order. They focus on the present,

and consequently their goals are temporary and replaceable, and their organizational means are valued as ends in themselves.

Third, present day social movements also rely on a new relationship between the latent and visible dimensions of their collective action. Social movements normally consist - here Melucci's work is at its most original - of "invisible" networks of small groups submerged in everyday life. These "submerged" networks, noted for their stress on individual needs, collective identity, and part-time membership, constitute the laboratories in which new experiences are invented. Within these invisible laboratories, movements question and challenge the dominant codes of everyday life. These laboratories are places in which the elements of everyday life are mixed, developed, and tested, a site in which reality is given new names and citizens can develop alternative experiences of time, space, and interpersonal relations. For Melucci, there is a complementarity between these "private" submerged networks and their publicly visible dimension. Movements appear relatively infrequently as publicly visible phenomena - for instance, during public demonstrations in favour of abortion or against nuclear power - and yet their involvement in observable political action is only temporary. Movements are only part-time participants in the public domain, precisely because they practise new forms of everyday life.

Fourth, and finally, contemporary movements are acutely aware of the planetary dimension of life in complex societies. Their emphasis upon the interdependence of the world system helps stimulate a new consciousness of ourselves as members of a human species which is situated in a natural environment. Melucci places considerable emphasis

on the peace and ecological movements, precisely because they are testaments to the fragile and potentially self-destructive connections between humanity and the wider universe. These movements publicize the fact that local events have global ramifications - that nuclear war, for example, would bring with it the end of civilization, and that every Chernobyl and chemical spill ultimately affects all individuals and their environment.

In summary, Melucci's analysis of social movements argues that the symbolic challenge they present is of the utmost importance. He comments on what he calls peace "mobilizations" - even they do not qualify as "movements" - as displaying no analytical unity. Rather, he suggests that they be understood as expressing the conflicts of complex societies, not just as responses to the threat of nuclear annihilation. Which begs the question; what, then, are these "conflicts"? His answer, interestingly enough, focuses precisely upon the issues that are the burden of this dissertation.

Contemporary societies are increasingly "informational", Melucci says, and as such constantly expand the realm of the artificial, the (electronically) "built" environment. Time and space are redefined in important ways so that, for instance, little room is left for "unifying the fragments of personal identity" (Melucci, 1989: 805). Moreover, with operational logic, information is not a shared and widely available resource, but rather is controlled by the few. Access to knowledge and information becomes a field of power and conflict. That Melucci sees nuclear war as an ultimate social intervention in an artificial world, important though it is, need not concern us here. The point is that the "social" realm becomes one of power, risk, and responsibility.

Melucci concludes that the analysis of social movements amounts to an analysis of ways that power is made "visible" under the conditions of "informational" societies. He warns against seeing such movements in overly-institutional terms. Rather, they are likely to work through temporary organizations, public campaigns, and "submerged networks" (Melucci, 1989: 813-14). He proposes that a key task for postindustrial democracy is to expand the arena of "public space", not for movements to become parties, but for their messages to be heard and translated into political decision making, without loss of autonomy.

This analysis provides a plausible framework for understanding the "Australia Card" example with which I started this section. And other cases, such as the Lotus "Household Marketplace" software, make sense within the same framework. This highlights the ways in which so-called submerged networks become temporarily visible and mobilize around a key issue, indicating that indeed countervailing forces against surveillance do exist, though not necessarily or always in the form of conventional pressure groups, lobby groups or political parties.

Some such relatively formal organizations do exist, of course, and play a crucial role, especially in providing background research when "significant events" occur. Prominent examples are the American Civil Liberties Union or the British group Liberty (formally the National Council for Civic Liberties). Other organizations, such as the Green Party in Germany, have made valuable contributions to surveillance and civil liberties debates, even though their main mandate lies elsewhere. (It should be noted that the German coalition groups against electronic identity cards failed to prevent their

adoption in 1987). In Britain and elsewhere, consumer groups have also joined forces with those questioning the assumed benefits of electronic surveillance, notably in relation to debt blacklisting and direct mail.

Another illustration of the dialectic of control, I think, is the proliferation of movements which themselves are computer networks to share their concerns. These include "Computer Professionals for Social Responsibility", the "Electronic Frontier Foundation", the "Electronic Privacy Information Center", and "Privacy International", which draws together data on electronic surveillance from widely scattered countries across the world. Such networking is likely to become increasingly important as a means of mobilizing appropriate assessments of surveillance by electronic media.

Lastly, the role of the mass media in providing analysis of surveillance is also significant. For example, throughout the debates surrounding Bill 68, several well-informed "specialists" within the Quebec media devoted themselves to the privacy cause (Boyer, 1996: 8). And in the rest of Canada and the United States, viewers have been exposed to detailed documentaries such as the "We Know Where You Live" programme on direct mail. Similarly, in Britain, a highly controversial series called "Secret Society" was screened by the BBC in 1987, including an episode on the "Zircon" spy satellite that was impounded by M15 from the BBC's Glasgow studios. Thus, in the context of "informational societies", where social cleavage occurs along non-traditional lines, journalism can become a source of alternative viewpoints.

Reasons for the Relative Lack of Public Resistance to Contemporary Surveillance

Melucci's arguments - summarized only briefly in the preceding section - provide a new framework for analysing social movements in contemporary western societies. However, they are deliberately open-ended and therefore leave many questions unanswered. For instance, Melucci recognizes the need to specify concretely the institutional processes of "complex" societies, and yet he fails to provide a convincing model of the kind of society we are living in. Moreover, his argument for new public spaces poses many difficult strategic questions: can the new cultural codes of movements - supported by organizations such as women's presses, alternative theatres, and small manufacturers of environmentally safe products - survive in a market dominated by large-scale economic and cultural enterprises? Doesn't the need for movements to seek political recognition and legal guarantees compel them to participate in political parties and state institutions, which at the same time threaten their very autonomy and survival? And finally, Melucci's framework, while informative and refreshing, makes no attempt at explaining why some modern institutions - and not others - seem to have provoked the forming of social movements that call them in question.

Capitalistic organization, for example, has been accompanied by the rise of labour movements, industrial expansion by Green movements, and so on. With regard specifically to surveillance, though, there is a relative lack of countervailing organizations committed to investigating, and if necessary, resisting its spread. I have already suggested one reason why this is the case. That is, many of the achievements of surveillance are viewed - rightly - as positive social benefits. Why resist systems whose advantages seem

to carry with them a number of acceptable risks? However, there are other important reasons for the relative lack of public resistance to surveillance, which I discuss in this section.

Resisting electronic surveillance, or at least attempting to channel it into ethically and politically appropriate directions, is important insofar as the chronic quest for personal data-collection that typifies modern life demands specific and urgent critical attention. Questions of justice and fairness must be raised when people's everyday activities are monitored and their habits, commitments, and preferences classified by the would-be omniscient organization. Such classification is both an outcome not only of social differences but of advantages and disadvantages, and often serves to reinforce inequalities of life-chances. And while it undoubtedly enables us to participate in society in numerous important ways, it also constrains us and encourages us to comply with the social order. The more marginal or nonconforming we are, the stronger the web of constraint-by-surveillance becomes.

Surveillance is thus a morally and politically loaded activity. As such, I have argued throughout the dissertation that if it is to be amenable to critique and to challenge, contributions are required from both those engaged in social analysis *and* those struggling directly with surveillance realities in the public policy arena. In terms of the former, it is important to understand that issues of social inequality and social control are connected with issues of trust and personal integrity. Particular forms of communication are a vital aspect of what it means to be human. What we disclose to whom, and under what conditions, is highly significant. What once we might have revealed, consciously, about

ourselves to someone we trust - a friend, doctor, priest or therapist - may now be involuntarily disclosed by electronic means to organizations or machines that we cannot know, let alone trust, in the same way. Thus, our identity is understood by others - and by inanimate machines - more from our data image than from our personal communication.

In other words, living in modern "surveillance societies" may throw up challenges of a fundamental - ontological - kind. Not surveillance as such, but the specific surveillance trends of the late twentieth century seem to raise questions for which as yet we have far from adequate answers. While it would be foolish to imagine that this dissertation provides such "answers", I hope that at least the questions are being made clearer. My own stance, which guides my choice between theoretical and practical alternatives, is nurtured by traditions of feminist, Christian thought. These call for care about all situations in which human dignity and justice are threatened. At present, the large "metaphysical" questions are all too frequently ignored (Fortner, 1986: 151-72), rather than engaged by a critical analysis based on specific views of justice and human personhood, as discussed in Part I of the dissertation.

Lastly, in terms of the public policy arena, groups or coalitions which argue for limits to electronic surveillance expansion are critical. Such organizations provide social scientists with the jolt of real-world situations and technological advances in a way that allow social theories to connect with what is actually happening in today's advanced, industrialized societies. As such, this section examines the history of what may be termed "counter-surveillance" movements, as well as comments on their present day status and achievements. In this regard, though, it is important to note that fundamental changes

which have taken place in society's approach to traditional privacy issues have hindered both the growth and effectiveness of counter-surveillance movements in recent years. Four factors that are central to these changes are also examined in this section, with particular emphasis on how these factors have retarded political activism over even the most blatant privacy invasions since the 1980s. The section concludes noting that these four trends are fundamentally changing the nature, scope, and relevance of privacy:

1. from privacy protection to data protection Formal rules in the form of data protection principles appear to have satisfied some of the concerns of information users and the public, but have failed to stem the growth of surveillance.

2. the creation of partnerships All stakeholders, whether proponents of surveillance or traditional opponents, have been transmogrified into a "partnership" with common goals and desires.

3. the illusion of voluntariness Many surveillance schemes now involve a "voluntary" component that has the effect of neutralizing public concern.

4. privacy rights as commodities Many traditional rights have been put on a commercial footing, thus converting privacy rights into consumer issues (as in the case of Caller ID blocking).

The Quantum Shift in Privacy Activism

In the early 1970s, with the advent of new information gathering techniques, a strong anti-census movement evolved throughout Europe. The protest in the Netherlands, for example, was so widespread that it achieved a critical mass that finally made the census unworkable. A substantial number of Dutch citizens simply refused to supply information

to the census authority (Flaherty, 1985). At that point in Dutch history, privacy achieved a notable place on the political agenda. In the wake of the census protest, a new organization called *Stichting Waakzaamheid Persoonsregistratiie* (meaning Privacy Alert) was formed. For the next twenty years, it provided a powerful and effective focus for privacy issues in the Netherlands.

However, in 1993 the fortunes of *Stichting Waakzaamheid Persoonsregistratiie* went into decline, and in 1994, the organization was dissolved. Although the decision by the Board of Directors to close down the organization involved financial matters, it also reflected changes in social attitudes towards privacy. It seems that the board was simply not committed enough to support the group through hard times, despite clear evidence that Holland was facing severe and widespread privacy problems. Indeed, the end of *Stichting Waakzaamheid Persoonsregistratiie* came at a time when the country was establishing new police and administrative powers motivated by the Netherlands partnership in the Schengen Agreement[59] - issues far more fundamental than the census.

Stichting Waakzaamheid Persoonsregistratiie was easily the world's most successful non-government privacy organization, yet it failed to survive the most crucial period of its history. Other organizations elsewhere have suffered the same fate, although alternative approaches to privacy protection have evolved in their place. For instance, the Canadian Privacy Council, despite a promising inauguration in 1991, has failed to

---

[59] The Schengen Agreement on police cooperation, which currently involves about half the countries in Europe, was designed to ensure that the dismantling of border controls did not happen at the expense of public and national security. The result was a strengthening of the powers of national police and authorities, and the development of the Schengen Information System to share data among countries.

materialize. However, in 1996 the Canadian Standards Association released a groundbreaking formal privacy standard, described in detail in Chapter Five. Similarly, the New Zealand Privacy Foundation, born in the heat of the campaign against the Kiwi Card, now exists only in name,[60] although the existence of the foundation motivated the government to enact a relatively strong and broad privacy law. In addition, the Australian Privacy Foundation, which organized a massive 1987 campaign against a national ID card, now serves only as a response mechanism, with few members and no budget. In its place is the Australian Privacy Charter, which - not unlike the Canadian situation - provides a more quantifiable approach to privacy issues (Davies, 1996: 154-55).

The loss of *Stichting Waakzaamheid Persoonsregistratiie* is an important symbol of changing times. With the sole exception of the Washington-based Electronic Privacy Information Center (EPIC),[61] privacy lobbies around the world are becoming less effective. Shifts in public attitudes have created new and complex challenges that privacy groups have yet to absorb. For example, since the mid 1980s, opinion polls have revealed a high level of concern about computers, but this has rarely translated into political action. Instead, most of the population has nurtured a symbiosis with information technology. Many consumers are prepared to surrender their personal data to information systems in return for the promise of a safer, cheaper, more efficient life. Additionally, the transmogrification of privacy rights into legal and consumer rights means that the slack is

---

[60] An inaugural meeting was held in Auckland on September 13, 1991.

[61] EPIC was formed in 1993 as a non-government watchdog over threats arising from electronic surveillance and censorship, and to champion a range of consumer, freedom of information, and privacy issues.

being taken up by institutional bodies, such as courts, industry watchdogs, and trading-standards bodies.

All this is not to say that many individuals and community groups are unconcerned about privacy issues. The Internet and related technologies, for instance, reflect a fertile ground for new forms of privacy activism. Among these are EPIC's electronic petition against the US government's Clipper Chip proposal, the use of web sites as a means of exposing the private lives of public figures who have opposed privacy protection,[62] and the use of electronic mail in "wildcat" strikes against privacy invading organizations. Nevertheless, traditional privacy activism at a macro political level has waned. From the perspective of privacy reform, this is a matter of deep concern insofar as the upsurge in surveillance by private and government bodies around the world shows no signs of abating in the near future.

Assessing the Four Fundamental Transitions in Privacy

It is tempting to assume that the demise of privacy activism is merely a sign of a natural shift in values. However, it is more likely that there are numerous causative factors which have been engaged by private and government interest groups, legal and intergovernmental organizations, and by the media.

---

[62] In July 1996 an anonymous website was established to convey "real-time" images from a camera placed outside the home of Defence Secretary Michael Portillo. The tactic, and the controversy which followed, succeeded in highlighting a contradiction in the frequently expressed government view that no right of privacy exists in public spaces.

1. From Privacy Protection to Data Protection

As European governments and international organizations such as the OECD, the European Commission, and the Council of Europe struggled from the early 1970s on to resolve growing fears about computers, a group of principles slowly evolved to form a basis for law. Data, according to these principles, should be collected, processed, and distributed fairly, accurately, on time, and with a measure of consent. In theory, the privacy of personal information was to be protected through these principles. In reality, however, such principles, as well as the regulators who enforce them, have had a limited impact on key aspects of surveillance.

There are two particularly serious problems associated with the core data protection principles. The first and most obvious is that they tend to allow a great many privacy violations to occur through exemptions for law enforcement and taxation. The second, and perhaps the graver problem, is that data protection law does almost nothing to prevent or limit the collection of information. Many acts merely stipulate that information has to be collected by lawful means and for a purpose directly related to a function or activity of the collector. Thus, a virtually unlimited number of information systems can be established without any breach of law.

As such, it would be a mistake to assume that data protection principles can address the most pressing privacy problems. In this vein, the Dutch privacy expert Jan Holvast recently explained that privacy legislation "corrects mistakes and misuses but it does not attack the way in which technology is used. On the contrary, experiences with data protection law in several countries show that these laws are legalizing existing

practices instead of protecting privacy" (1991). Similarly, Privacy International observed in its 1991 report: "Protections in law, where they exist, are sometimes ineffective and even counter-productive. Extensive information holdings by government are invariably allowed under exemptions and protections in law. The existence of statutory bodies, rather than impeding trends, sometimes legitimates intrusive information practices" (1991: iv).

In addition, data protection acts are seldom privacy laws. They are *information* laws, protecting *data* before *people*. Instead of being concerned with the full range of privacy and surveillance issues, they deal only with the way personal information is collected, stored, used, and accessed. In Britain and Australia, for example, these laws are generally not concerned with visual surveillance, drug testing, use of satellites, or denouncement campaigns (e.g., hotlines for reporting tax dodgers). Finally, many data protection acts do not cover publicly available information such as land titles and electoral rolls that are available for general public inspection.

Thus, data protection acts generally have serious limitations. Nevertheless, I would insist that they are tremendously important. Without relaxing my indictment of them for being cynical, sieve-like, and subject-unfriendly, it may still be said that such laws are a necessary minimum. Weak law is better than none at all. Precedents for some protection are set that way, and the foundation for improvements laid. In addition, in a situation where surveillance becomes increasingly global, it is interesting to note that legal limits start to have international implications. The European *Data Protection Directive*, for instance, will have beneficial effects on citizens beyond Europe, as well as within it.

As Europe requires trading partners to comply with the directive, Canada (and hopefully the United States) will be obliged to extend legislation to the currently untouched field of consumer surveillance.

2. Subjects in Surveillance Are Becoming Partners in Surveillance

The new generation of closed-circuit television (CCTV) surveillance equipment currently in use in Britain comes closer to the traditional perception of Big Brother than any other modern surveillance technology. There are now linked systems of cameras with full pan, tilt, zoom, and infrared capacities. Among the more sophisticated technological features of these systems are night vision, computer-assisted operation, and motion detectors that place the system on red alert when anything moves in view of the cameras. The clarity of the pictures produced by these systems is often excellent - many are able to recognize a cigarette pack at 100 metres. Additionally, the camera systems increasingly employ bullet-proof casings and automated self-defence mechanisms. They can be legitimately described as military-style systems transplanted to an urban environment.[63] If any technology was to provoke the ire of a community, this should be the one. In Britain, however, the reverse is true.

Britain's CCTV schemes have embraced an important promotional element, resulting in 200,000 cameras covering public spaces and a growth rate of 20 to 30 per cent annually for the surveillance industry. To give the CCTV systems added weight and appeal, they are invariably promoted as partnerships, with all stakeholders recast as

---

[63] These systems were pioneered in the 1970s at Scottish defence establishments, such as the Faslane submarine base.

investors or shareholders. These new partners usually include police, local businesses, the town council, community groups, the media, the insurance industry, and "the citizens". This strategy parallels other schemes, such as "partners against crime" and "community partnerships" in Canada and the United States. Thus, the flavour of much modern anti-crime advertising in Europe and North America is one of togetherness: "Crime . . . together we can crack it" and "Working together for a crime free America" are typical slogans. Partnerships are also a common element in "neighbourhood watch" schemes, which require a certain level of participation.

The "partnership" or "shareholder" model brings together parties who traditionally would have been in opposition. In this regard, it may help different parties to work towards a common goal. For example, in the "investor" or "partner" process, parties are part of an inclusive formula that embraces all the major elements of a project. Inherent in the model is the implication that all stakeholders are integral to planning, are equal partners in the outcome, and are overall winners in the scheme of things.

However, the "partnership" or "shareholder" model has two serious disadvantages from a privacy reform point of view. First, there is the implication that contributions from non-stakeholders are invalid. For instance, proponents of the CCTV schemes in Britain routinely portray critics as enemies of the public interest who are more concerned with personal privacy than with controlling crime or reducing urban dysfunction. Second, there is the problem of "function creep", which occurs as more partners participate in surveillance projects, thereby raising the stakes. For example, although originally installed to deter burglary, assault, and car theft, most CCTV camera systems have been used to

combat "anti-social" behaviour, including minor offences such as littering, drunkenness, urinating in public, traffic violations, fighting, obstruction, and evading meters in town parking lots. They have also been widely used to intervene in underage smoking and a variety of public-order transgressions. According to a Home Office promotional booklet entitled "Looking Our For You", CCTV technology can be a solution for vandalism, drug use, drunkenness, racial harassment, sexual harassment, loitering, and disorderly behaviour (Home Office, 1994: 12).

Thus, innovative uses are constantly being discovered for CCTV technology. As such, CCTV camera systems are now an integral part of crime control policy, social control theory, and "community consciousness" in Britain, despite the fact that their effectiveness in preventing crimes is uncertain. As more and more partners have a stake in the face of crime prevention and social control, CCTV camera systems are an increasingly attractive investment. In fact, many central business districts in Britain are now covered by them. Their use on private property is also becoming popular. And this form of surveillance may even extend to the home. For instance, Andrew May, Assistant Chief Constable of South Wales, has urged victims of domestic violence to conceal video cameras in their homes to collect evidence (Hencke, 1997). Finally, the technology is already being used in hospitals to support covert surveillance of parents suspected of abusing their children.

3. The Illusion of Voluntariness

Many surveillance schemes now involve a "voluntary" component which has the effect of neutralizing public concern about surveillance. For example, when the Cardiff

police in Britain were searching for the murderer of a young girl in 1995, they asked the entire male population of a local housing estate to "volunteer" DNA for testing - "just so we can eliminate you from our enquiries", each was assured. The reality was that anyone who did not "volunteer" was considered a suspect and was therefore subject to special scrutiny.[64] In the same year, this tactic was used by the London police after the rape of a girl on Great Portland Street. In that case, police had written to local residents with certain physical characteristics, again arguing that volunteering for the DNA test would "eliminate" them from further enquiries. Also in 1995, the drivers of all Mercedes trucks of a certain colour throughout England were subject to the same "request".

In some regions of surveillance, governments seem less inclined to make privacy invasion mandatory, choosing instead to say that participation is a matter of free choice in an open market of services. Shortly before the British government was to issue a Green paper on a national ID card, for instance, cabinet papers were leaked revealing that the dominant view among planners was that police and civil rights concerns could be resolved if the ID card was made "voluntary". In May 1995, the Home Office released its Green Paper on the ID card. The document offered numerous models for a card scheme, including voluntary cards, multi-purpose cards, and compulsory cards, in several formats. No particular format was recommended, though the document appeared to give special weight to a multi-purpose system compulsory only for benefit claimants and drivers (e.g., 90 percent of the population). For the remainder, the card would be "voluntary".

---

[64] *Daily Telegraph*, London, April 4, 1995.

The British government appears to have taken a lead from the Australian experience with ID cards. In Australia, the architects of a national ID card used the expression "pseudo-voluntary". Although it was not technically compulsory for a person to obtain a card, it would have been extremely difficult to live in society without one. There is some anecdotal evidence that this pseudo-voluntary approach may have the effect of neutralizing privacy concerns (Davies, 1992). It might be widely viewed that those who do not "volunteer" bring problems upon themselves.

This prospect could be exemplified by an international biometric handprint-registration system for passport holders. If such a system were to be imposed by force, it would most likely result in a political scandal. Instead, it has been introduced with great success as a voluntary system. The project, called INPASS (Immigration and Naturalization Passenger Accelerated Service System), has been operating since 1993 as a voluntary system for frequent travellers. More than 65,000 travellers have so far enrolled in the system, a figure that increases by almost 1000 a week. Governments in 26 countries are coordinating with the project.

If the INPASS trial is successful, the technology may ultimately make conventional ID cards and passports redundant. In exchange for faster processing, passengers will have to accept a system that has the potential to generate vast international traffic in their personal data. Ultimately, a universal immigration control system may be linked to a limitless spectrum of information, including the data in police and tax systems.

It is ironic, in view of even a notional element of privacy, that people tend not to support more privacy friendly technological options that are less likely to collect damaging

personal data. According to several sources, the signs are not good. Customers using smart cards, for example, tend to prefer a full accounting of the goods and services they purchase. And similarly, when smart cards are used to calculate road tolls, people are often anxious to make sure they have not been shortchanged (Schuster, 1994). In this regard, one US assessment of public responses to road toll technology observed (Schuster, 1994):

> Concerns that motorists would feel their privacy was compromised under an ETTM [Electronic Toll and Traffic Management] system which recorded vehicle movements prove to be unfounded. Toll agencies that record this information do not make it available to outside parties. In fact, existing ETTM experience reveals that a large majority of motorists choose payment options (often via credit card) which do not provide anonymous transactions.

4. Privacy Rights Are Becoming Commodities

Today, people may rightly be disturbed at the discovery that personal data about them circulates well beyond their reach within some government department or consumer corporation; rightly, if it is agreed that personhood and self-identity are violated by involuntary disclosure, and that relations of trust are made more fragile thereby. But an increasingly common response is to claim not just certain rights to oversee or control the circulation of personai data, but actually to *own* them. In societies that have rapidly commodified information as a means of perpetuating social control through consumerism, it comes as no surprise that people believe that they possess their data image.

For example, in the United States, a group of householders, feeling themselves beleaguered by junk mail, have formed an organization called "Citizens Incorporated". They turn the tables on the telemarketers by attempting to bill companies for the use of

their domestic telephone, time, and personal details.[65] Similarly, others have proposed that property rights be established over the commercial use of personal data. Brokering firms would handle such rights on behalf of their clients, operating the enterprise on similar computer networks as those used by the direct marketers. The quantity of unsolicited mail would diminish while its quality would rise (Rule, 1990: A8).

This kind of approach is also advocated by well known privacy advocate Alan Westin. In testimony given before an American House of Representatives Subcommittee on Government Information, he interpreted results of the 1990 Equifax Survey on Privacy. Between what Westin calls "privacy fundamentalists" and "greatly concerned", is a group of "unconcerned" people whose views could swing either way, depending on a number of factors. Because he cannot decide why individuals might trade privacy for consumer benefits, Westin proposed that the market should decide. For instance, corporations could make special offers to those willing to cede control over personal information, thus making so-called privacy fundamentalists pay higher prices. For Westin, this constitutes "a highly responsive and democratic way of institutionalizing consumer choice" (Gandy, 1991).

This debate will no doubt continue and intensify as the value of personal information rises along with public awareness about what is happening. However, it is my opinion that attaching an economic value to privacy forces this interest to compete and defend itself in the market place. This effectively shifts the grounds of the privacy debate

---

[65] As depicted in the production "We Know Where You Live", Coronet/Nova Films, 1991.

from a discussion of social values and priorities to a crass consideration (calculation) of individual economic interest. Furthermore, the completely free market alternative seems to me to invite abuse, analogous to the case of the poorest selling their blood in countries where this is permitted. True, we already inhabit societies where personal data are commodities, and where some people - but not, it is noteworthy data subjects - are profiting from their sale. But can this unfairness be redressed, and some measure of control over personal data be regained by data subjects, only by instituting a system of "royalties"? In my view, such a quest would simply disadvantage the less well-off.

Thus, the process of commodification is inimical to privacy. Every element of privacy protection is interpreted and promoted as a direct cost to the consumer. Additionally, though, privacy's journey from the political to the consumer realm reflects a more disturbing trend in privacy activism: rather than exploring the deeper meaning of privacy in relation to communication, self-identity, and thus human dignity, privacy is located in the economic sphere. The upshot of this is that privacy is understood as a matter of self-protection. Those who are aware that data protection and privacy laws exist, and who have the resources and motivation to take advantage of them, may do so. Furthermore, those with entrepreneurial initiative may take up arms against commercial surveillance by declaring property rights over "their" personal data. However, it seems to me that this simply extends the early modern focus on self-protecting individualism. So although privacy was in the early modern period a privilege of the ruling classes, only later becoming identified with the non-public realm, one could justly argue that we have come

full circle: privacy is a privilege once more, with little attention being paid to its human dignity and self-identity aspects.

The Challenges to Surveillance: Technical and Mobilization Responses Revisited

The concept of privacy has shifted in the space of a generation from a civil and political rights issue motivated by polemic ideology to a consumer rights issue underpinned by the principles of data protection and by the law of trading standards. In other words, privacy has metamorphosed from an issue of societal power relationships to one of strictly defined legal rights. Several mechanisms have played important roles in this shift. First, opposing players have been recast as "partners" in surveillance. In addition, privacy invasion has often been accompanied by the illusion of voluntariness. And finally, private rights and public interests have been subtly but substantially redefined. This chapter has discussed these shifts in detail as well as commented on how they have created new and complex challenges that privacy groups have yet to absorb.

On the latter note, this chapter has argued that in many countries - particularly throughout Europe - traditional privacy activism has declined. This is vastly different from the situation in the 1960s and 1970s, where the privacy movement was fuelled by a strong spirit for the protection of democratic rights. In the present day context, though, privacy is divorced from its roots in issues of sovereignty, technophobia, power, and autonomy. Instead, privacy protection is widely perceived as constituting a set of technical rules governing the handling of data. Consequently, privacy advocacy has been recast as a legal and a consumer rights issue. The upshot of this is that while there are

now more codes, conventions, and laws in place than ever before, more data on more people is being collected by more powerful systems and for more purposes than at any other time in history - with minimal public discussion or resistance.

Thus, increased public awareness of surveillance issues is critical. As such, I have looked at recent challenges to surveillance, in the form of legal limits and mobilization responses. As noted in Part II, the former contains some vital principles, and serves to provide some buffer against abuses. However, most privacy and data protection laws also tend to be minimalist, ambiguous, and geared to permitting citizens to protect themselves. Mobilization responses, on the other hand, differ from technical responses in that they attempt more radical questioning and opposition to the perceived negative consequences of surveillance practices. They relate to social movements (Melucci), and are often spurred by technological developments such as Caller ID, smart cards, and national identification systems.

Unfortunately, though, we have seen that mobilization responses in the last ten to fifteen years have rarely translated into more permanent and powerful manifestations of resistance. Which brings us to the question of what else can be done? In this regard, I suggest that there are four possible alternatives for increasing public awareness of surveillance issues.

First, educative initiatives should be welcomed. In the United States, for example, university and college computer science accreditation requires the inclusion of "social and

ethical implications of computing".[66] Second, public awareness of surveillance issues could be raised through professional groups and organizations, especially those directly concerned with computing, information management, and so on. For instance, recall the dramatic results of the Electronic Privacy Information Center and Computer Professionals for Social Responsibility in blocking the release of the Lotus "Household Marketplace" software in 1993. Their attempts to argue for limits to consumer surveillance expansion fit in exactly with my criteria of *participation*, *personhood*, and *purposes* outlined in Part I of the dissertation. Resisting the growth of electronic surveillance *per se* would be a futile gesture. Attempting to channel it into ethically and politically appropriate directions is much more *a propos*.

Third, and more broadly, other kinds of movements may also contribute to the containment of surveillance. If we are to think of "surveillance as a site of struggle in its own right" (Giddens, 1990), then there is every reason to expect various kinds of groups and movements to contest this territory, no doubt in the name of privacy. Consumer groups and organizations represent one important sector which has already flexed its muscles. Similarly, in Britain banking practices and consumer blacklisting have come under criticism, and in the United States more *ad hoc* groups have mobilized to resist unwanted direct marketing.

Needless to say, the political problem involves not only identifying agencies that might spur transformative activity, but also searching for appropriate ways of doing so. It

---

[66] See, for instance, materials from the Research Center on Computing and Society at Southern Connecticut State University.

is clear, for instance, that some kinds of regulation of surveillance practices could wind up with as much invasive bureaucratic machinery as the practices they intend to reduce. It is also equally clear that if surveillance is not to be viewed in a paranoid fashion, then space must be made not only for viewing it as a "necessary evil" but as a "greater good". Caller ID telephone services is a case in point. Technical means are available for maintaining such services for women or minority groups in danger while denying them to direct marketers. The question of which purposes would be better served is critical here.

Which brings us back to one of the main arguments advanced in the dissertation, as well as my fourth alternative for increasing public awareness of surveillance issues. Surveillance should be a major concern of both social analysis *and* political action because it has become a central feature of contemporary advanced societies. In terms of the former, I have offered the three categories of *participation*, *personhood*, and *purposes*, described in Part I of the dissertation, as a means by which the normative content of surveillance theory may be weighed, and by which new theory may be devised. In terms of the latter, such categories could find a role within political practice at the movement/mobilization level discussed in this chapter. For example, consumers and citizens show that they are far more knowledgeable than certain deterministic theories allow. However, I am also going to suggest that these categories have already found a role within an entirely different field - breast cancer - and that by studying this field, privacy advocates and scholars may be able to do some "lesson-drawing" (Bennett, 1990) for their own pursuits in raising public consciousness about surveillance.

I have chosen to focus on the field of breast cancer because much can be learned about the politics of privacy from the analysis of other political fields. And breast cancer is a highly charged political field, particularly since 1990. In that year, geneticist Mary-Claire King narrowed the search for a gene for heritable breast cancer to a stretch of a single chromosome, fairly guaranteeing that someone would locate it in the next few years. In 1991, Dr. Susan Love, a frustrated surgeon; Susan Hester, whose companion had died of the disease; and Amy Langer, Executive Director of the National Alliance of Breast Cancer Organizations, cofounded the National Breast Cancer Coalition, a lobbying group bent on obtaining increased funds for breast cancer research. In 1992, Congress appropriated an unprecedented $210 million for a new research program, to be administered by the army. And in 1993 the Clinton Administration embarked on a National Action Plan on Breast Cancer, to define for the first time in the United States a national strategy for research and health care. Finally, in 1994, BCRA-1, the gene for heritable breast cancer that King had spent her life looking for, was found. Thus, a new science, a new advocacy movement, and a new political commitment were born.

By studying these "births" - or what may be termed the political rise of breast cancer - I demonstrate in the next chapter that the field of breast cancer activism is rich in lessons about raising public awareness, not only of health issues but of others as well. Thus, I situate privacy as a comparative political issue. By examining privacy in this way, it is possible to examine wider propositions about the formation of public policy, the choice of policy instruments, and the implementation and evaluation of policy decisions, not only with regard to privacy but more widely as well.

Chapter Seven: Public Awareness Movements

Lesson Drawing from the Breast Cancer Awareness Movement

In the last seven years, funding for breast cancer research and treatment in the United States has increased dramatically - from $90 million to $500 million annually (Stabiner, 1997). There is also a National Action Plan on Breast Cancer, designed to establish a national health care strategy and identify research priorities, that has been in effect since 1993. In addition, heightened awareness about breast cancer has been achieved through three national signature campaigns, which collected 600,000 signatures in 1991, 2.6 million signatures in 1993, and another 2.6 million signatures in 1997 (Altman, 1996). In short, breast cancer has become the focus of national attention and policy in the United States, reaching even the level of the Presidency.[67]

In Canada, breast cancer is also a public issue, commanding both increased funds and attention from the media. For example, the Canadian Breast Cancer Research Initiative has funnelled $31 million into research projects on breast cancer since it was founded in 1993 (Nichols, 1998). And a recent *Maclean's* cover story on women's health opened with an article on breast cancer treatment and attitudes, and included a separate section on funding for breast cancer research in Canada (1998: 52-63).

The recent rise in breast cancer awareness, in both the United States and Canada, is rooted in two factors. First, there is the collision of technology and the population curve. Improved mammography equipment and advanced biomedical technologies have enabled doctors to detect more cancers. At the same time, the baby boomers are aging,

---

[67] The Clinton administration held a meeting in December 1993 to establish a National Action Plan on Breast Cancer. The president's own mother died from breast cancer in 1994.

and as they do, their risk of breast cancer increases. As more women from this generation have gotten sick - and died - from breast cancer, the media have taken notice.

Second, increased public awareness about breast cancer can be attributed to the work of activists in this area, particularly in the United States, where the breast cancer awareness movement was founded. In the 1970s and early 1980s, the standard treatment for breast cancer was a mastectomy followed by radiation and chemotherapy; the "slash, burn, and poison" regimen as it was commonly known - and criticized - by breast cancer activists (Love, 1990). In addition, the only formal support program available for women with breast cancer in 1970 was the American Cancer Society's "Reach to Recovery Program", in which a visit from one of the program's volunteers had to be requested by a woman's doctor, not the woman herself. And in 1981, the National Cancer Institute's budget for breast cancer research was $33.9 million, almost ten times smaller than its 1995 budget of $323.7 million (Altman, 1996: 27-28).

Since the 1970s and early 1980s, however, breast cancer has been redefined as a national public issue, "a social malady that has eaten at the integrity of the American family, and has done so for far too long" (Stabiner, 1997: 17). Breast cancer has even been declared a national epidemic - 182,000 women get breast cancer every year in the United States and 46,000 die. Between 1990 and the year 2000, it is estimated that nearly half a million women will have died from the disease. Finally, the economic implications of breast cancer have been recognized by President Clinton, who stated in a speech to breast cancer activists and the media that there was "no excuse for why we would spend

so much money picking up the pieces of broken lives, when we could spend a little bit of money trying to save them" (Stabiner, 1997: 17).

In October 1993, the President set forth his plan. The Secretary of Health and Human Services, Donna Shalala, would hold a meeting to establish a National Action Plan on Breast Cancer in December 1993. The plan would establish a national health care strategy, research priorities, and political policy to outlast the Clinton Administration's commitment to breast cancer awareness. The plan also promised a new emphasis on prevention and improved methods of early detection. Doctors around the country would offer discount mammograms in observance of National Mammography Day. And the plan would include payments for screening mammograms for women over fifty, as well as any woman under fifty whose doctor specifically recommended a mammogram. In the space of a generation, then, breast cancer had been redefined; the disease was no longer a secret shame, to be endured without complaint, but a national public issue commanding widespread media attention and increased funds for research and treatment.

This chapter examines this re-definition process. In so doing, it argues that activist groups are capable of taking definitional capabilities upon themselves and changing the domains within which these definitions are discussed. In the case of breast cancer, activists have changed the definition of breast cancer from a private women's health issue, to a national public issue with significant social and economic costs (Altman, 1996). That is, they have demonstrated that definitions can be shifted from the *private* to the *public* domain. This is important in that power is at issue here, and in quite complex ways (Kress, 1986). To assign an event to the sphere of the private is at once to declare it void

of power, and to assign responsibility to individuals. It is to offer an account of that event which says that there is no account other than individual action and expression. To assign an event to the sphere of the public, on the other hand, is to assert that it is beyond individual responsibility and within the domain of social control. The public is then the domain of the action of social, political, and economic forces, and of persons acting not as individuals, but as social agents in social roles.

In the 1970s and early 1980s, breast cancer was defined in the private realm. The disease was shrouded in silence because losing a breast was viewed as losing a defining portion of one's femininity, which was seen as a private matter. For example, Mary Jo Kahn, an activist from the Virginia Breast Cancer Foundation, states (Altman, 1996: 299):

> In my mother's time, breast cancer was an embarrassment because the disease was clearly tied up in sexuality. When my mother got breast cancer, she felt like she was no longer a woman. She was kidded by her friends. It was America's difficulty in dealing with sexuality on all issues that prevented us [breast cancer activists] from getting concerned twenty years ago.

The link between breast cancer and sexuality is important in that it relegates the disease to the private realm where, to borrow from Kress (1986), it is outside the social and inside the domain of individual expression. In the 1990s, however, breast cancer no longer centered on a woman's sexuality, but was associated with gender inequality in health care and with severe social and economic costs (Altman, 1996). This relegated breast cancer to the public realm, which meant that it was beyond individual responsibility and within the domain of social control. As a result, today breast cancer is no longer viewed as a private, woman's health issue.

The shifting of issues from the private to the public domain, where they can be subject to social responsibility and control, is important for those concerned with increasing public awareness about surveillance. In current policy debates about privacy, it has generally been assumed, if not explicitly argued, that threats to privacy invade an individual (private) interest and that privacy protections are individual (private) rights (Regan, 1995). When privacy is defined in this manner, policy formulation entails a balancing of the individual right to privacy against a competing interest or right. In general, the competing interest or right is recognized as social (public). As a result, privacy has been put on the defensive, with those alleging a privacy invasion bearing the burden of proving that a certain activity does indeed invade privacy and that the "social" benefit to be gained from the privacy invasion is less important than the individual harm incurred. If the terms of the policy debate are to be shifted, privacy thus needs to be reconceptualized in a way that sustains wider interest and support; that is, it needs to be redefined in the public domain. Breast cancer activism provides a case study as to how this can be achieved.

However, breast cancer activism is not only instructive in the shifting of definitions from the private to the public domain. Throughout the dissertation, I argue that surveillance has become a major feature of contemporary, advanced societies and as such, it should be the focus of both social analysis *and* political action. This chapter focuses on the latter by demonstrating how those struggling directly with surveillance realities in the social and political arenas might benefit from the experiences of breast cancer activists. In this regard, breast cancer activists have been successful in two other social processes:

pressure group organization and media use. This chapter examines these other processes, following from the work of Alberto Melucci (1989), as discussed in Chapter Six, and Gunther Kress (1986).

In terms of the former theorist, I argue that in a society increasingly shaped by information and signs, social movements play an important role as messages or symbols that express oppositional tendencies and modalities. This is most evident in the peer group organization that breast cancer activists have formed with diverse groups. In terms of the latter theorist, I examine how the media constantly assert the existence of the public and private domains, and how they assign events to one domain or another. This means that the media have control of access to the domains of public and private. I examine this control and its relation to activist discourses. Thus, this chapter analyses the success of breast cancer activists in *three* social processes: the definitional reconstruction of issues; pressure group organization; and media use.

Lesson Number One from Breast Cancer Activists: Definitional Reconstruction of Issues

Breast cancer activism is fundamentally concerned with criticizing existing social and medical definitions of breast cancer. But, unlike the privacy awareness movement, breast cancer activists have successfully challenged the status quo. That is, they have organized systematic opposition to standard treatments, research budgets, and public attitudes towards breast cancer; whereas opposition to electronic surveillance expansion has been of a far more limited and muted kind. In order to determine why this is the case,

it is necessary to examine how breast cancer has been redefined in the 1990s as a national public issue, primarily by breast cancer activists. Breast cancer, I have already suggested, is no longer a private, woman's health issue associated with the loss of femininity, but is now seen as a health equality issue. Because health equality is a public issue associated with ideas about money and power, the disease has been redefined in the public domain. As such, it is now beyond individual responsibility and is subject to social control.

This definitional shifting from the domains of the private to the public is the basis for any successful public awareness movement, and provides an important lesson for privacy activists. In the late twentieth century, the range of surveillance settings has increased dramatically, and surveillance capacities are expanding in each dimension. New categories of social relationships are emerging in relation to the data image, and social divisions, especially those articulated with consumption, are being reinforced. If this "surveillance society" is to be challenged, then privacy needs to be reconceptualized in a way that sustains broad interest and support; that is, it needs to be redefined in the public domain.

The redefinition of breast cancer is rooted in three areas, each of which are examined in this section: (1) changes in medical practices towards breast cancer treatment; (2) the rise of local breast cancer support and advocacy groups; and (3) the rise of national breast cancer awareness organizations. By examining each of these areas, it is possible to trace the evolution of breast cancer from a woman's disease, and a source of private embarrassment and shame, to a national public issue.

(a) Changing breast cancer treatment practices

Women have been getting short shrift in health care for years. For example, in 1979, a study on the medical treatment of women versus men found that doctors treated men and women who complained of the same symptoms differently (Armitage, 1979). Doctors were more likely to refer male patients for diagnostic tests and to attribute women's complaints to stress or hypochondria. The same study also found that female patients were twice as likely as men to have the abnormal results of an exercise test blamed on "psychiatric or other noncardiac causes". Additionally, it was shown that women were less likely than men to receive kidney transplants, have coronary bypass surgery, or have their lung cancer diagnosed. The study concluded that "there is evidence that physicians are more likely to perceive women's maladies than men's as the result of emotionality" (1979: 33).

In addition to different treatment from men, women's health concerns have a history of being dismissed or just plain ignored. A Louis Harris poll for the Commonwealth Fund in 1993 found that 25 percent of the women surveyed said they had been "talked down to" or treated like a child by a doctor compared with 12 percent of the men surveyed (Louis Harris and Associates, 1993: 7). And 17 percent of women compared with 7 percent of the men questioned were told by a doctor that a condition they thought they had was "all in their head". Speaking at a breast cancer conference in May 1994, former National Institutes of Health director, Bernadine Healy, M.D., stated that, "women who have chest pains are not treated the same as men unless tests show they are having a heart attack" (Stevens, 1995: 12).

Similarly, an article in 1993 on women's experiences with the silicone breast implant revealed that "the issue of having women's concerns about medical problems heard and respected is not new and persists in contemporary society" (Merkatz, 1993: 22). The study's authors also found many similarities between the way the silicone breast implant and the Dalkon Shield, an IUD device, were handled. In both cases, it took widespread publicity to finally generate investigations, which resulted in the removal of the two products from the Canadian and American markets. In both cases too, many women who experienced health problems were not taken seriously by their physicians, and their symptoms were not acknowledged by the manufacturer. The Dalkon Shield and the silicone breast implant represent two of the most popular medical devices for women in modern times. If women's complaints had been listened to and taken seriously early one, the problems with these devices may have been found years sooner and many women would have been spared unnecessary suffering.

Finally, the historical medical treatment of women also features their exclusion from major medical studies. Rebecca Dresser, a bioethicist at Case Western Reserve University's medical school, writes about the lack of women in medical trials and provides the following examples (1992):

* The relationship between low-cholesterol diets and heart disease "has almost exclusively been studied in men".
* Evidence that aspirin can prevent some migraine headaches was produced in studies on men even though women suffer from migraines up to three times more often than men.

* Studies of AIDS treatments frequently omit women, despite the fact that women represent "the fastest growing infected population".
* A recent study of the possible relationship between caffeine and heart disease involved over 45,000 men and no women.

There are several reasons why women have been excluded from major medical studies, despite growing evidence that life threatening illnesses manifest themselves differently in men and women (Altman, 1996). For years, men dominated the power end of the medical field - they were the doctors and scientists, so they chose to study other men. Additionally, many women were excluded from medical studies on the basis of pregnancy, or possible pregnancy, under the assumption that the developing fetus might be harmed. (That same risk has also kept women from getting jobs in some businesses and industries.) And finally, it was believed that women's hormonal changes would complicate medical studies (Todd, 1993: 96).

The exclusion of women from major medical studies has put them at a distinct disadvantage when it comes to their health. As such, the National Institutes of Health (NIH) released a policy statement in 1986 urging applicants for research grants to include women and minorities in clinical trials or to have a good reason for excluding them. It was the right direction, but unfortunately not one that was taken by many researchers. Later, in 1989, the Congressional Caucus for Women's Issues pointed out that women's health problems accounted for only 13.5% of spending by the NIH (Altman, 1996: 19) and called on the General Accounting Office (GAO) to study the exclusion of women in medical research at the NIH (Monroe, 1993: D15). In June 1990, the GAO issued its

report, which found that medical research was (still) being done mainly on men, and that the NIH had been inconsistent in implementing its policy, which called for encouraging the inclusion of women in clinical trials (GAO, 1990: 1-106).

After the release of that report, a revised NIH *Guide for Grants and Contracts* was published in August 1993 (NIH, 1993: 29). It stipulated, among other things:

* The number of women included in a study would be proportional to their prevalence in the condition being studied.

* If the correct number of women were not included, the investigator's ability to answer the questions posed would be compromised, unless an appropriate justification were provided.

* There would be peer review of any justification given for not including women; if it were not considered appropriate, that would be factored into the final recommendation of approval or disapproval and the level of relative merit given to the proposal.

* Studies which exclude women would have to have compelling justification to do so to be awarded funding.

At the same time, the Office of Research on Women's Health (ORWH), which was created by the NIH in 1990, identified breast cancer as one of its top priorities for the 1990s. In addition, Bernadine Healy, M.D., became the first woman to head the NIH, and within a week of her confirmation announced preliminary plans for a $500 million study of women's health problems, known as the Women's Health Initiative (WHI). The proposal supported her earlier testimony before a congressional subcommittee that "one of the compelling reasons why we need a major interdisciplinary study of women's health is

because of the enormity of the breast cancer problem among American women".[68] Not surprisingly, among the issues in women's health problems to be evaluated were the genetic, dietary, and other risk factors associated with breast cancer.

Unfortunately, the results of the WHI, and its potential answers about the link between breast cancer and suspected carcinogens, are at least ten years away. In the meantime, though, the WHI is significant in that it represents the transformation of breast cancer from a silent epidemic to a national public issue. In this regard, the historical medical treatment of women, and the anger breast cancer activists have expressed about it, is paramount. For example, Health and Human Services Secretary, Donna Shalala, has stated

> The truth is that the changes we see in our federal budget for breast cancer research, the changes we see in the national media attention focused on breast cancer, and the changes this administration has made to increase resources for breast cancer have been motivated in large part by the power and anger of women all across this country.[69]

Similarly, Amy Langer, the Executive Director of the National Alliance of Breast Cancer Organizations, talks about a "new" kind of breast cancer patient - "one who is involved in charting the course of her care, but also angry, frustrated, and amazed that we have not made more progress against this disease" (Altman, 1996: 313).

---

[68] Hearing before the House Committee on Government Operations Subcommittee on Human Resources and Intergovernmental Relations, November 12, 1990.

[69] Conference to Establish a National Action Plan on Breast Cancer, December 16, 1993.

Thus, the historical medical treatment of women with breast cancer has pushed women into redefining the disease, particularly as the incidence of breast cancer has increased. Since the 1990s, activists have refused to be an afterthought to the mostly male medical and political establishment. Instead they are fighting to ensure that in the first decade of the new century, the number of women dying from breast cancer will dramatically decline.

(b) The rise of local breast cancer support and advocacy groups

In the late 1970s and early 1980s, local support and advocacy groups specifically for women with breast cancer were started. Before that time, "breast" and "cancer" were two words that one did not utter in polite company, either singly or together. But as support and advocacy groups started to grow all over the United States, women with breast cancer began talking openly about their illness. In these groups, patients compared the different treatments they were getting and gave each other hints about what to do about side effects such as nausea and hair loss. They also exchanged information on different doctors and encouraged each other to switch doctors if necessary. The groups thus did a great deal to "demystify" breast cancer and empower women. In this regard, they "played the greatest role in the development of the breast cancer advocacy movement" (Altman, 1996: 294).

The accomplishments of local breast cancer advocacy groups are noteworthy. In May 1979, for example, Massachusetts became the first state to pass an informed consent law for women undergoing a surgical biopsy which means, in effect, that a two-step surgical procedure is now required. If a woman's biopsy proves to be positive, she can

then research her treatment options before making a decision regarding a second surgical procedure. The exception is the woman who signs a consent form allowing her doctor to perform whatever surgery he or she feels is necessary after getting preliminary results from a biopsy. Informed consent cannot be obtained from a woman who is unconscious or on the operating table.

On May 20, 1992, Massachusetts also became the first state to declare breast cancer an epidemic and to launch a campaign to fight the disease. It announced a three part plan, following from guidelines released by the Massachusetts Breast Cancer Coalition: (1) pilot education programs to reach poor, uninsured women who don't get regular medical checkups; (2) a bill that would require state licensing of mammography facilities; and (3) improved surveillance, by the state, of the incidence of breast cancer. Finally, in Springfield, Massachusetts, activists marched to demand that breast cancer reconstruction be included in women's medical coverage. The state's Blue Cross and Blue Shield plans had refused to cover the procedure, calling it cosmetic. Activists countered with the argument that breast reconstruction was "rehabilitation" and should be covered just the way penile and testicular implants in men had *always* been covered (Kahane, 1993: 52). The activists won.

In California, an informed consent law was passed in 1981 following the efforts of breast cancer patient/activist, Juliet Ristom. Before Ristom was even definitively diagnosed with breast cancer, her doctor had reserved an operating room for a mastectomy. When she asked about alternatives, her doctor refused to give her any other information. She did her own research and eventually chose a lumpectomy, keeping her

breast. In a letter to members of the California Assembly, she said that she had taken control of her treatment, and that all women should have equal opportunity under the law to do the same.

Ristom and the California Breast Organizations (CABCO) were also instrumental in getting a special "breast cancer check-off" on the state income tax for breast cancer research. Under the check-off, a person can indicate a certain amount of money to be used for breast cancer research when filing a tax return. A special research fund has been set up, with patient advocates on its board. In its first year, the check-off raised over $300,000. Another, and potentially far richer, source of income in California is the two-cent-a-pack cigarette tax enacted by the California Assembly. The money generated by this levy will fund breast cancer research, awareness, and education.

In short, then, the gains made by local breast cancer advocacy groups are far-reaching. The foundation for these gains, however, was actually laid in the 1970s, long before breast cancer had become a national public issue. At that time, feminists began to urge women to understand their own physiology and to take control of medical decisions previously reserved for physicians. In 1973, the book, *Our Bodies, Ourselves*, by the Boston Women's Health Collective, was published. It challenged women to take responsibility for their health care and gave them the information they needed to do so, particularly in the area of reproductive health. Later in the 1970s, feminist consciousness raising groups encouraged women to see their particular problems as part of a larger pattern of discrimination and inequality, an idea which was emphasized in the milestone book, *Breast Cancer: A Personal History and Investigative Report*, by Rose Kushner.

Kushner, an ardent feminist and patient/activist, published the book in 1975 and was "one of the most persuasive and expressive advocates for women with breast cancer".[70]

In addition to the feminist movement, local breast cancer advocacy groups were also inspired by the AIDS awareness movement, which had successfully demonstrated that passive acceptance could be changed into words and actions. Amy Langer argues that "women have traditionally played the role of private patient, private caretaker, and discreet employee but that we have seen with AIDS that those who are able to speak out and transform the personal to the political have had some measurable effect".[71] In a similar vein, Ellen Hobbs of Save Ourselves (SOS) in California, suggests that "if breast cancer activists did the same thing as the AIDS activists and got real noisy, they'd get the money too".[72] Finally, Susan Claymon, co-founder of Breast Cancer Action (BCA), notes that BCA tried to make contact with friends in the AIDS awareness movement:[73]

> I believe that we were the original advocacy group to say, 'Hey, the AIDS movement has done some great stuff. It's changed the way the American medical system works. They've brought the patient into the process.' And patients' intimate knowledge of AIDS has become a very valuable commodity in the research and legislative worlds. These were people who weren't trained scientists but who taught themselves well and kept educating themselves well. So we wanted to learn from them and do the same kind of thing for breast cancer.

---

[70] "Breast Cancer: Race for the Cure," Hearing before the House Subcommittee on Health and Long Term Care of the Select Committee on Aging, May 16, 1990.

[71] Telephone call with Amy Langer on January 19, 1998.

[72] Telephone call with Ellen Hobbs on January 19, 1998.

[73] Electronic message from Amy Langer received on January 20, 1998.

Although breast cancer and AIDS are both health issues, the fact that activists for the former could "borrow" from activists for the latter indicates that lessons may be drawn from one public awareness movement and applied to another. In this regard, I offer suggestions later in the chapter on how the privacy awareness movement might "borrow" from the breast cancer awareness movement in the area of definition construction in different realms. In the meantime, though, it is important to note that breast cancer activists learned from AIDS activists how to redefine private suffering as public anguish. That is, they learned to emphasize the social and economic ramifications of breast cancer by showing how women with the disease often faced problems with health insurance, job discrimination, and sexual relationships. Thus, like AIDS activists, breast cancer activists were able to alter minority perceptions of their disease, and broaden the terms under which it was publicly discussed. As such, they were able to lay the groundwork for a formal national action plan on breast cancer.

(c) The rise of national breast cancer awareness organizations

It is actually national breast cancer awareness organizations, rather than local breast cancer support and advocacy groups, who are formally responsible for the Clinton administration's National Action Plan on Breast Cancer. Until 1990, breast cancer activists focused primarily on the patient's need for information and services. At that time, the major advocacy group at the national level was the National Alliance of Breast Cancer Organizations (NABCO), an umbrella group run by Amy Langer, a breast cancer survivor, to serve as a resource for patients around the United States. Women depended on NABCO for everything from information on clinical trials to advice on where to buy a

wig. What was lacking, though, was a national organization that challenged the government's research agenda. That required a shift in focus, from the patient community outward.

That shift came in December 1990 when Langer met with breast surgeon Susan Love, at that time the director of the Faulkner Breast Centre in Boston, and Susan Hester of the Mary-Helen Mautner Project for Lesbians with Cancer, in Washington, D.C. They discussed the possibility of starting a coordinated effort to fight breast cancer. The idea was to have breast cancer patients lobbying on their own behalf for things such as research, legislation, and regulations. The coalition was to be comprised of local breast cancer advocacy groups from all over the United States. Langer contacted Diane Blum of Cancer Care, Sharon Green of Y-ME, and Nancy Brinker and Linda Cadigan of the Susan G. Komen Foundation, and suggested that they all meet sometime in late January 1991 as a "first step in organizing a joint effort". In her December 17, 1990 memo, Langer wrote, "Although each of our organizations has been active in some aspects of patient advocacy, I feel we can accomplish more, faster, if we work together".[74]

Two months later, on February 28, there was an announcement that a national breast cancer advocacy coalition was being formed. The planning groups were NABCO, Y-ME, Cancer Care, the Faulkner Breast Centre, the Mautner Project, and the Women's Community Cancer Project (WCCP). The press release listed three major objectives of the organization, to be called the National Breast Cancer Coalition (NBCC): (1) to promote *research* into the cause of, cure for, and optimal treatments for breast cancer

---

[74] Memo supplied by Amy Langer.

through increased funding, recruitment, and training of scientists and improved coordination of funds distribution; (2) to improve *access* to high quality breast cancer screening, diagnosis, treatment, and care for all women, particularly the underserved and uninsured, through legislation and beneficial changes in the regulation and delivery of breast health care; and (3) to increase the involvement and *influence* of those living with breast cancer in the areas of legislation, regulatory processes, and all aspects of clinical trial design, including access to trials. The announcement concluded by saying, "Breast cancer patients and their supporters will be invited to participate in national and local grass roots advocacy efforts on behalf of American women, all of whom are at risk for developing breast cancer".[75]

The first major undertaking of the NBCC was "Do the Right Thing", a letter writing campaign. Its goal was to generate 175,000 letters that would go to members of Congress and President Bush, asking them to show their support of breast cancer-related legislation and regulation. The goal of 175,000 letters represented the number of new breast cancer cases projected for 1991. In the end, some 600,000 letters were collected. Fran Visco, president of the NBCC, says that the 600,000 letters "told us it would be a success, that there was a real movement out there waiting to happen" (Altman, 1996: 317). The outpouring of letters resulted in an appropriation of $132 million for breast cancer research to the National Cancer Institute for fiscal year 1992 - a gain of almost 50 percent over 1991 spending.

---

[75] Telephone call with Fran Visco on January 15, 1998.

Since that time, the NBCC has become the largest and most effective political organization for breast cancer in the United States. In February 1992, for example, at a Senate appropriations committee hearing on the NIH budget, Fran Visco listened to one health activist after another ask for a bigger piece of the budgetary pie. The answer was always the same: If we give more money to you, then we have to take it away from someone else. So, when it was Visco's turn to speak, she decided to try a new tactic. She told the senators that she did not want a bigger piece of the pie, but a bigger pie: "You'll just have to look for more money for health care. You managed to find the money when it was time to bail out all those white guys in suits from the savings and loan crisis. Are you saying now that you can't find money to fight breast cancer?" (Stabiner, 1997: 61).

Her strategy was successful. Despite the strenuous resistance of many senators who argued that medical research dollars belonged in the NIH and domestic programs, Senator Tom Harkin introduced a "stealth amendment" to appropriate $210 million (1 percent) of the Department of Defence budget for breast cancer research for fiscal year 1993. Furthermore, Congress allocated an additional $25 million for fiscal year 1994, and in October 1994 allocated $115 million in the army's 1995 budget for breast cancer.

Since the vote on the "stealth amendment", the NBCC has enjoyed other triumphs in the fight against breast cancer, mainly by emphasizing the severe social and economic costs of the disease. For example, during speeches to policy makers, coalition activists have pointed out that the cost to the U.S. economy in 1993 for women diagnosed with breast cancer was approximately $23.1 billion, with business sharing over $10.2 million of that cost according to an analysis based on data from the National Cancer Institute

(Altman, 1996: 27). Those costs include medical treatment and the loss of productivity and earning because of premature death. In addition, there are indirect costs associated with breast cancer including a general deterioration of quality of life for patients as well as for family members, friends, and coworkers. Finally, the disease can result in anxiety, reduced self-esteem, resentment, family conflicts, antisocial behaviour, and even suicide. By emphasizing these costs, NBCC activists have been able to successfully redefine the disease as a national public issue worthy of widespread media attention and increased funds for research and treatment. As such, they have continued to achieve many important objectives in their fight against breast cancer.[76]

What Privacy Activists Can Learn

Breast cancer activists are potentially helpful to privacy activists because they have demonstrated that the reconstruction of issues from the domains of the private to the public is the key to the success of any public awareness movement. For example, the success of the breast cancer awareness movement is due to the ability of activists to redefine breast cancer as a national public health issue with significant social and economic costs (Altman, 1996). In this regard, breast cancer activists have successfully challenged thinking about traditional notions of public and private. That is, they have long deplored the lack of seriousness with which breast cancer, and a woman's "private" shame and fear surrounding it, have been treated by public authorities. As such, they have argued convincingly for public intervention in this "private" matter, noting that while privacy may connect closely with freedom for men, for women - especially those with breast cancer -

---

[76] See http://www.natlbcc.org/goals/htm.

there is less reason to be sure of this. Breast cancer activists have thus shifted the demarcation line between what issues are to be included in the public domain, and hence deserving of public responsibility and action.

This is of immense importance to matters considered in the dissertation for two reasons. First, many privacy activists and scholars are insensitive to feminist critiques of privacy. There has been extensive debate among philosophers and legal theorists about what privacy means, whether and how it can be defined, and the scope of protection it can and should afford. Reactions to recent court cases in both Canada and the United States have made it clear that many in the public are unwilling to give up the privacy protection they currently enjoy (Bennett, 1996 and Decew, 1997). They view privacy as a valuable shield for protecting a sphere within which a person can act free of scrutiny and intrusion from others. In contrast, many feminists have called attention to the "darker side of privacy", citing its potential to shield domination, repression, degradation, and physical harm to women and others without power (Decew, 1997). Perhaps the most prominent version of this critique of privacy is articulated by Catherine MacKinnon who observes (1989: 187):

> By staying out of marriage and the family - essentially meaning sexuality, that is, heterosexuality - from contraception through pornography to the abortion decision, the law of privacy proposes to guarantee individual bodily integrity, personal exercise of moral intelligence, and freedom of intimacy. But have women's rights of access to those values been guaranteed? The law of privacy instead translates traditional liberal values into the rhetoric of individual rights as a means of subordinating those rights to specific social imperatives.

For MacKinnon, the move to ensure privacy in intimate relations with respect to the body, home, and family does nothing to help women since the values of individual

bodily integrity, exercise of moral intelligence, and freedom of intimacy are not guaranteed to women. The fundamental flaw, according to MacKinnon, is that underlying privacy protection in the law is a liberal ideal of the private: as long as the public does not interfere, autonomous individuals interact freely and equally. But this presumes that women are, like men, free and equal, an assumption that MacKinnon and other feminists find patently false (Allen, 1988; Gavison, 1992; Olsen, 1985, and Pateman, 1989). Thus, for these feminists, privacy law fails to recognize and take into account the preexisting oppression and inequality of women.

This, of course, relates to breast cancer activism in that activists for this cause have argued persuasively that to the extent that breast cancer was relegated to the private domain, it was held unavailable for public scrutiny or intervention. When breast cancer was redefined in the public domain, though, the history of neglect surrounding the disease could no longer go unchecked. This is not to say that the public domain fails to exhibit the social power of sexism, as breast cancer activists have demonstrated, for example, with respect to women's long-standing exclusion from major medical studies (Altman, 1996). The subordination of women to men is still evident in the public sphere, and in the private sphere it is mirrored and allowed to run its course, "inaccessible to, unaccountable to . . . anything beyond itself" (MacKinnon, 1989: 190). My point, however, is that there exists a traditional notion of a public (male) political realm and a private (female) domestic realm, and that issues are treated differently depending on the realm in which they are defined.

At present, privacy is defined and defended in the private realm and as such, it risks keeping women isolated and politically powerless. In other words, characterizing a

realm of domestic, personal, intimate, and familial relations as private sustains and increases existing unfair power relationships and opportunities for abuse. Nevertheless, there may be great value for women, as well as for men, in preserving a "private" sanctuary where a person can live free from "public" scrutiny and the pressure to conform. This clearly represents a challenge to many of the aforementioned feminists, some of whom are willing to jettison privacy completely.

As an alternative, I suggest that if the full consequences of a surveillance society are to be understood and their challenges met, then something other than a legislative approach to privacy will be necessary. An educative process is also required, as well as the mobilization of opinion and action on a number of fronts. This is where breast cancer activism is particularly instructive because it has demonstrated that the long term solution to the disease lies in such intangible areas as *participation*, *personhood*, and *purposes*. We may recall that these categories were introduced in Chapter Three as a means of finding hope in the field of surveillance, which is dominated by dystopic paradigms.

In terms of *participation*, for example, both local breast cancer advocacy groups and national awareness organizations have argued persuasively for the maximum involvement of their members in the research process, including decisions on major medical trials. In terms of *personhood*, we have seen that breast cancer activists have challenged the historical medical treatment of women and its ties with the "maleness" of enlightenment epistemologies that emphasize the controlling rather than the caring, and the rational at the expense of the emotional. Through events such as the Annual Advocacy Training Conference, the "Face of Breast Cancer" art exhibitions, and the "Do

the Right Thing" letter campaigns, breast cancer activists have cleared space for alternative models of understanding and action predicated on the "humanness" of breast cancer patients rather than on their significance as mere medical cases or statistics. Finally, in terms of *purposes*, breast cancer activists have suggested that their disease should be the constant subject of public scrutiny and political concern. This is because of the ease with which such purposes may be subverted, obscured or replaced. The story of breast cancer in North America is laden with references to pessimism, paternalism, and neglect. As such, the alternative for activists has been to identify people and projects whose purpose is not just to eradicate the disease, but also to redefine traditional medical practices and to redirect the ways in which issues involving women are usually relegated to the private domain, whereas those affecting men tend to be defined as public.

The three categories of *participation*, *personhood*, and *purposes* are, therefore, important because they have helped to shift the definitional markers that signify whether breast cancer discourses are discussed in the domains of the private or the public. It remains to be seen, however, whether such categories will perform the same function in the privacy awareness movement. In Chapter Three, I suggested some preliminary ways in which these categories might contribute to alternatives to today's surveillance difficulties, and they are worth repeating here.

For instance, in terms of *participation*, I noted that the emphasis in future privacy laws - such as the Canadian privacy legislation for the private sector - could be shifted away from mere (private, individual) self-protection towards placing a greater onus on data-gatherers (in the public domain) to ensure that data are obtained fairly, and in the

demonstrably best interests of data subjects. In terms of *personhood*, contemporary surveillance systems could be constructed in ways which include (public) social goals with caring and protective motifs. For instance, records could be erased when no longer needed thereby demonstrating the (public) social goal of forgiveness. To achieve this, groups of professionals, from systems designers to quality controllers, would have to be involved (Smith, 1994). Finally, in terms of *purposes*, a concentration on *limits* would be apt. For example, one limit, highly pertinent to an era in which the use of new technologies is serving to blur the boundaries between previously discrete domains, would be a sphere-by-sphere check on surveillance operations. What may be ethically or politically unassailable in one sphere is often inadmissible in another (Regan, 1995).

At the beginning of this section, I stated that breast cancer activists have shifted the demarcation line between what issues are to be included in the public domain, and hence deserving of public responsibility and action. I suggested that this is an important idea for privacy activists and scholars for two reasons. First, it is important for a feminist critique of privacy, as I have just discussed. But it is also important in that most privacy activists and scholars fail to underscore the public importance of privacy, and instead focus on its legal basis as a private, individual right (Regan, 1995). This provides a weak basis from which to formulate effective privacy or data protection law because it entails the balancing of a private, individual right to privacy against other competing rights, which are usually defined as social or "public". Usually, these social or "public" rights "provide a stronger engine for policy change or the basis for political mobilization" (Regan, 1995: 211).

For example, Priscilla Regan documents how rights defined as social or "public" were able to defeat privacy rights, which were defined as "private" or individual, in three major court cases in the United States concerning information privacy, communications privacy, and psychological privacy (1995: 174-211). In each of these cases, Regan notes that the ideas competing against privacy had broad appeal - efficiency of government operations in the case of information privacy, law enforcement and national security in the case of communications privacy, and the reduction of theft and fraud in the workplace in the case of psychological privacy. As a result, privacy was put on the defensive, with those alleging a privacy invasion bearing the burden of proving that a certain activity did indeed invade privacy and that the "social" benefits to be gained from the privacy invasion were less important than the individual harm incurred. If the terms of the policy debate are to be shifted in the future, privacy thus needs to be reconceptualized in a way that sustains wider interest and support; that is, it needs to be redefined in the public domain. Breast cancer activism provides a case study as to how this can be achieved by demonstrating that the demarcation line between what issues are to be included in the public domain can be shifted by activist groups through their use of the three categories of *participation*, *personhood*, and *purposes*.

Lesson Number Two from Breast Cancer Activists: Pressure Group Organization

When Dr. Marie-Claire King first began her search for a heritable gene for breast cancer in the 1970s, the government was the dominant source of funding for medical research. However, by the time the National Action Plan on Breast Cancer was

announced in 1993, two of King's postdoctoral fellowships depended on the Susan G. Komen Foundation for sustenance. Times had changed. The advent of managed care, which meant dwindling profits from patients, and the U.S. government's growing budget crisis, had translated into fewer public dollars for medical research. As a result, breast cancer researchers were forced to look for ancillary sources of cash.

They found them in two sources - private philanthropists and corporate sponsors. The U.S. government's disregard for breast cancer research until 1991, coupled with the size of the demographic group at risk for the disease, had opened the field to entrepreneurial interests eager to invest in what looked like a promising future. As such, several companies began to sponsor genetic research into the heritable gene for breast cancer. For example, in 1991, Eli Liliy & Co., the Indianapolis-based pharmaceutical giant, bought the licensing rights to future gene tests for breast cancer from Myriad Genetics Inc., a biotechnology company founded by breast cancer researcher Mark Skolnick in Salt Lake City, Utah for $1.8 million. By 1993, similar ventures had become the norm.

There was a time, though, when researchers were reluctant to accept money from pharmaceutical companies or other private sources because it branded a scientist as a second-string researcher, one who had to go begging for funds because their own government did not consider them qualified for a research grant. The funds were perceived as tainted; it looked as if the researcher was working for the company, whose drug or equipment they were testing, rather than working for the "truth". It was difficult to tell the company that wrote the cheques that its medicine did not work.

Today, however, those old prejudices have fallen away, casualties of financial need. The annual cost for breast cancer treatment is estimated to be seven times the cost of health care for women without the disease. And, over a twenty-seven month period, the average cost in the United States is estimated at $34,000, although in some cases the bill can exceed $345,000 (Chambliss, 1994). Breast cancer is big business. Any word of a possible breakthrough in a chemotherapy agent now sends pharmaceutical company stock prices soaring. When the drug gets FDA approval, its manufacturer can usually look forward to an increase of profits in the millions. As such, the researchers who have private money seem clever, even progressive, both for having figured out a way around a strangled federal budget and for possibly being able to share in profits from things such as future gene tests and therapies.

The money from private philanthropists and corporations that has been attained for breast cancer research is due in large part to the work of activists. In fact, activists played a critical role in lobbying for research dollars, particularly from companies that had no prior history of supporting women's health issues. For example, the National Alliance of Breast Cancer Organizations (NABCO) lobbied General Electric to sell mammography machines, and Du Pont to sell the film that the machines required, thereby making possible early detection on a wide scale (Osimo, 1997: 9). In addition, activists from Cancer Care, a national breast cancer support and advocacy group, succeeded in convincing the British chemical company Imperial Chemical Industries (I.C.I) to found breast cancer awareness month, along with the American Academy of Family Physicians in 1988 (Panter, 1997: 29). Finally, NABCO urged Zeneca, the United States subsidiary of I.C.I, to donate

tamoxifen citrate to a government-funded prevention trial for women with a high risk for breast cancer (Panter, 1997: 30). Tamoxifen citrate is a synthetic hormone used to prevent breast cancer recurrences and was discovered and developed by Zeneca.

However, the assistance provided to breast cancer research and detection programs by the aforementioned companies was not necessarily altruistic, as noted by many breast cancer activists. General Electric and Du Pont, for instance, both have high numbers of hazardous waste sites. Similarly, I.C.I. produces an array of chlorine-based products including pesticides, paint, and plastics. In 1990, the United States federal government filed a major chemical dumping lawsuit against six defendants, including I.C.I. American Holdings Inc., accusing them of dumping millions of pounds of DDT and PCBs into the Pacific Ocean between 1947 and 1971 - organochlorine chemicals that some researchers suspect of increasing breast cancer risk. The lawsuit was later dismissed on technical grounds by a judge who referred to environmentalists as "do-gooders and pointy heads" (Stabiner, 1997: 76). Breast cancer activists were quick to condemn the decision (Dekong, 1997: 11). And, finally, much to the dismay of breast cancer activists, Zeneca manufactures a carcinogenic herbicide, acetochlor. Annual sales of this product are about $300 million, whereas annual sales of Zeneca's Nolvadex, its trade name for tamoxifen citrate, are almost $400 million (Snedeker, 1997: 7).

Breast cancer research is thus prepared to ignore blatant ironies in the name of potential progress, for there is simply no other way to survive. In light of this, though, breast cancer activists have argued persuasively that anyone is welcome to join the fight against the disease, even those that are on the "hit list" of suspected contributors to

environmental risk (Lynn, 1997: 23). In fact, by working with those contributors, breast cancer activists have demonstrated the power of diverse peer group organization. In this sense, they are redolent of Melucci's characterization of social movements as a "sign" or "message", as described in Chapter Six.

For instance, the breast cancer awareness movement not only raises questions about women's equality and rights in health care. It also, at the same time, signals the importance of recognizing how social discourses are able to turn a private initiative into a public issue. For Melucci, this is indicative of the existence of free spaces between the level of political power and everyday life in which actors can consolidate collective identities through both representation and participation. As such, the symbolic challenge that the breast cancer awareness movement presents is of the utmost importance since it can be understood as expressing the existence of these spaces, and not just as a conventional political response to the threat of disease. In this way, new social movements thus emphasize the socially constructed nature of the world and the possibility of alternative arrangements.

The possibility of alternative arrangements is also embodied in the peer group organization that breast cancer activists have formed with companies that have nothing to do with medicine, such as those found in the pharmaceutical industry, and everything to do with women. For example, Revlon's Ronald Perelman has made a five year commitment to breast cancer gene research, and was one of the major sponsors of the National Breast Cancer Coalition (Stabiner, 1997: 76). Similarly, Evelyn Lauder, daughter-in-law of the founder of the Estee Lauder cosmetics empire, helped raise $20

million to underwrite the Evelyn Lauder Breast Center, which opened at New York's Memorial Sloan-Kettering Cancer Center in October 1992 - the same month that Lauder and *Self* magazine launched the pink ribbon as a symbol of breast cancer awareness (Stabiner, 1997: 76). In addition, designer Ralph Lauren, who knew *Washington Post* fashion editor Nina Hyde for seventeen years, led a fund-raising effort for a centre at that city's Georgetown University when Hyde was diagnosed with breast cancer in 1985 and complained that it was difficult to figure out how to acquire the best care (Stabiner, 1997: 76). And finally, "as a company that cares about the total well-being of women everywhere",[77] Avon has created its own Breast Cancer Awareness Crusade. Its mission is "to provide women across the United States, particularly those who are medically underserved, with access to a full range of breast cancer and early detection screening devices".[78] Since its founding in October 1993, the crusade has raised over $22 million, making it the largest corporate funder of non-profit breast health organizations in America.

The peer group organization that breast cancer activists have forged with so-called "woman-friendly" companies, and with those in other industries, indicates the diversity of the breast cancer awareness movement. Additionally, however, this peer group organization supports Melucci's argument about the political status of new social movements. Melucci's stance is that not only are new social movements *not* political, but rather that it is just as well that they are not. If the new movements were more political in

---

[77] See http://www.pmedia.com/Avon/back/background.html.

[78] See http://www.Avon.com/about/awareness/crusade.html.

the conventional sense of the term, they would be playing by sets of rules that benefit existing power-holders and they would in all likelihood be much easier to co-opt through normal channels of political representation and negotiation. Hence, their apolitical or antipolitical stance should be regarded as a strength rather than a weakness.

However, to be apolitical in this sense does not mean a retreat into excessively individualist orientations for Melucci. Although he operates with a culturalist reading of new social movements, he also believes that such culturalist movements pose major challenges to existing social relations. This is because these relations have come to be defined more and more in the cultural language of symbolic representation. Thus, if power has become congealed, particularly in media messages and administrative rationality, the most profound challenge to such power may come from cultural movements that challenge these messages and rationality. In this vein, diverse peer group organization among breast cancer activists challenges traditional social and medical definitions of breast cancer through symbolic discourses which have changed the domains within which the disease is defined.

What Privacy Activists Can Learn

Breast cancer activists are potentially helpful to privacy activists because they have demonstrated the power of diverse peer group organization. In other words, following from Melucci, they have shown that the socially constructed nature of grievances cannot necessarily be deduced from a group's structural location. For example, one would expect companies whose products may contribute to an environmental risk for breast cancer *not* to be receptive to breast cancer activism;

however, we have seen that the opposite is true. In terms of privacy activism, this is important because it may be possible to convince those who are invading privacy to become partners in protecting it. This is the corollary of an argument I made in Chapter Six, namely that subjects of surveillance are becoming partners in surveillance.

There are a few examples, although small in scope, of privacy invaders becoming privacy protectors.[79] The most recent are the new amendments in online marketing to the Code of Ethics and Standards of Practice released by the Canadian Direct Marketing Association (CDMA) in the fall of 1997. These amendments, which were drafted in consultation with privacy activists, require CDMA members to be clear as to what personal information they are collecting from online sources and how such information will be used. The amendments also require CDMA members to seek consumers' consent before sending them marketing e-mail.

This is similar to the "opt-in" approaches used by some publishing companies and other direct marketers in the United States. This approach allows individuals to "opt-in" to programs in which their personal information will be sold or used in additional ways. The choice between "opt-in" and "opt-out" approaches has significant implications. Direct mail experience, for instance, indicates that only about 20 percent of people make use of the "opt-out" option, that is, requesting that their information not be used for another purpose other than the original one for which it was collected; while it is estimated

---

[79] The most common examples are the privacy codes of practice discussed in Chapter Four.

that an "opt-in" option results in only about 5 percent giving their consent for further uses of their information (1990: 1, 26).

One of the major reasons why "opt-out" options are so popular with direct marketers and others is because of the rapidly growing role of the so-called information commodity. In this vein, William Melody, working within the perspective of Harold Innis, suggests that what distinguishes contemporary, advanced societies from their modern predecessors is the relation of information to the market (1986). The technology-led capacity to supply huge amounts of information in digital form has coincided with the discovery that such information often has a huge market value. In other words, data can command a price as a commodity. As Melody observes, "information that was previously outside the market and not included as economic activity has now been drawn into the market" (1986: 7). Thus, it is possible to see why many privacy invaders, who depend on the information commodity, are reluctant to participate in privacy protection schemes that may threaten their competitive advantage in an increasingly global, capitalist system.

The rapidly growing role of the information commodity has two facets, both of which are central to understanding the difficulties in constructing diverse peer group organizations with privacy invaders. First, large corporations - the data entrepreneurs - are involved in huge operations that easily match the scope of some government databases. Such corporations have frequent recourse to military analogies for their strategies, and constantly seek technological innovations that will support and upgrade these strategies. The power of the data entrepreneurs is highly asymmetrical with respect to individual consumers, or even privacy activists, who often lack the knowledge, will, or

organization to effect any resistance or change. In this regard, the rejection of the Lotus "Household Marketplace" software, described in Chapter Six, may represent the glimmerings of raised consciousness, but to claim more for it would be unrealistic. And it remains to be seen whether debates over new technological or legal innovations, such as smart cards in British Columbia or Quebec or the impending Canadian privacy legislation for the private sector, will do more for such raised consciousness in the future.

The other facet of the information commodity is that in consumer surveillance terms it is constituted by a particular kind of data image. Statistical digestion of data digitally culled from diverse sources provides data entrepreneurs with profiles of consumers as members of certain crudely defined social groupings. Others, based on individual identification, depend on data such as the all-important credit rating, not merely to distinguish between different types of consumers - gender and ethnic background loom large here - but to form judgements as to who is credit-worthy and who is not.

These sorting mechanisms may clearly be understood in panoptic terms, but not only in panoptic terms. For instance, while consumer surveillance surely does exhibit panoptic traits - unverifiable observation, behavioural classification, and so on - the actual mechanism of social integration and criterion for social participation relates to individual "free choices" made in the marketplace. Discipline may be present, but certainly not the carceral, coercive discipline of the panopticon. As such, it is difficult to convince the public that partnerships with privacy invaders are necessary, since these invaders are usually associated with the pleasure of consuming, rather than with the pain or coercion of

Panoptic discipline. This is the indirect means of soft social control which I described in Chapter Three.

Much hangs, of course, on this soft social control within the consumer marketplace. For example, discussion of surveillance capacities, with its negative connotations, might seem quite inappropriate in a sphere dominated by the discourse of "free choice". The illusory aspects of this have to be exposed, however, and this is where privacy activists are critical. For instance, privacy activists have pointed out that under the guise of greater choice, the cost of basic services - such as cable TV - is frequently driven up by artificially constructed "choices". Caller ID offers another illustration. Privacy activists have noted that customers within CLASS service areas may be offered both Caller ID facilities and the opportunity for their number not to be displayed to those they call, and that each of these carries a price tag. By exposing these hidden assumptions on which the social order of consumerism operates, privacy activists are able to clear ground for more responsible peer group organizations with privacy invaders. In so doing, they may be able to challenge the peculiar threat of consumer surveillance to exacerbate social division and undermine human dignity in the name of individuality, wideness of choice, and consumer freedom.

Lesson Number Three from Breast Cancer Activists: Use of the Media

Gunther Kress argues that the media, as crucial political and ideological institutions, have a major regulatory function in relation to the domains of public and private, and of the vast array of social classifications associated with them (1986). Their

function, according to Kress, is to participate decisively in the reproduction of both domains, which means that the media have control of access to the domains of public and private. As such, they are crucial to activist groups who are attempting to change the domains within which an issue is defined.

In the case of breast cancer, activists for this cause have changed the definition of the disease from a private women's health issue to a national public issue with significant social and economic costs (Altman, 1996). That is, they have demonstrated that definitions can be shifted from the *private* to the *public* domain. The media have been instrumental in this shifting in that they have formed a kind of synergy with breast cancer activists, who, in the early 1990s, began to feed journalists with medical reports and statistics as well as information on private and public events designed to increase public awareness about breast cancer (Altman, 1996 and Stabiner, 1997). For instance, on October 18, 1993, more than one thousand members from the National Breast Cancer Coalition (NBCC) participated in a televised march from the National Museum of Women in the Arts to the Ellipse, behind a coalition banner with the message "End the Breast Cancer Epidemic". At the same time, two hundred coalition members met with President Clinton, Hillary Rodham Clinton, and Health and Human Services Secretary, Donna Shalala, in the East Room of the White House to present the signatures from the second "Do the Right Thing" letter writing campaign.

In 1994, leaders from the NBCC helped to redefine and increase the visibility of breast cancer as a "national health emergency" by appearing on *The Today Show*, CNN's *Sonya Live*, and ABC's *Nightly News*. In 1995, the NBCC developed "Project Lead", an

innovative science program for breast cancer activists designed to educate them in basic scientific language so that they can participate on research boards and committees. In 1996, the NBCC hosted the first annual breast cancer think tank meeting, designed to "shake up the world of breast cancer", and generate new ideas to end the epidemic. And, finally, in 1997, the coalition hosted its first "Workshop for the Media: Understanding Breast Cancer Research and Policy". The workshop was directed to members of the media who report on breast cancer and was designed to give them the tools they need to critically analyse breast cancer information. Thus, breast cancer activists recognize that the media regulate access to the domains of private and public, and as such, they are the *main* definers of how activist discourse "is classified in relation to the domains of public and private" (Kress, 1986: 399).

The discourses of breast cancer activists, which the media have classified in relation to the public realm, bring to the public a greatly needed awareness of breast cancer. At the same time, though, it is the mass media, run for the most part by white, heterosexual males, which persistently promote the young, beautiful, and generally "busty" woman as the most attractive, as the woman who gets the most desirable man capable of providing all that is important in life. A woman's role, as defined by the media, has always been one of dependence on a male, and to get that male she must be more attractive than her competitors. In this vein, sociology professor Allan Mazur states, "the self-image of woman is not complete without her breasts, particularly in our society, where significant emphasis is placed on the female chest as portrayed on television, in magazines, and in

newspapers. We actually worship the female breast and when a woman has a breast removed, she loses one of her more important identifying features" (1986: 77).

Similarly, breast cancer activist Rose Kushner gives the media substantial credit for the obsession with breasts in North America (1984: 102):

> The media were responsible for the long hours my sons spent discussing who was a 32A or a 34B and, wonder of wonders, the fifteen-year-old who had a 40D. The media are the main reason my daughter and her girlfriends who, at the age of twelve or thirteen, stood before their mirrors trying to make the bumps in their training bras larger with the help of cotton balls, Kleenex, or ripped nylons. Male chauvinism plays an important role in all aspects of breast cancer, from the moment a sixth-grader's budding chest bumps make her popular, to the belief (many times correct) that breasts are vital to getting and keeping a boyfriend. The 'importance' of breasts is constantly reinforced by the media.

Kushner's comments reveal that it is impossible to talk about breast cancer, and in particular, its impact on a woman's sexuality and body image, without bringing up the role of the contemporary media. Conformity to the latest body image, reinforced by the mass media, is considered crucial to many women. The "Official Breast", as described by Naomi Wolf in *The Beauty Myth*, is constantly promoted by a culture that values the illusion of youth above the endless variety of the real world (1991). At the same time, "newspapers, magazines, television, and radio have educated the public about breast cancer, and the controversy surrounding some of its treatments" (Kushner, 1984: 44). As such, breast cancer activists have had to cope with a difficult contradiction: while their use of the mass media enables them to redefine the disease in the public realm, those same media also participate in the relentless public analysis of women's physical form. The relationship between breast cancer activists and the media is thus contradictory. In this

vein, Karen Stabiner, author of *To Dance with the Devil: The New War on Breast Cancer*, argues (1997: 114):

> No matter what the media says about breast cancer, there is always the other issue: how a woman feels about her breasts. They are her vanity, her sex life, her motherhood, an outward symbol of an attractive and useful self. When a woman loses a breast, the most mundane fact of life becomes an effort. She can no longer get up and get dressed in the morning without thinking about it. She cannot bathe or make love without being reminded of it. And even when she does forget, the media are quick to insist that she remember.

What Privacy Activists Can Learn

This contradictory relationship with the media, whereby the media function partly as a public educator and partly as a promoter of ideal standards for female beauty, is pertinent to modern surveillance contexts. On the one hand, for instance, privacy activists depend on the media to educate the public about surveillance. In the popular press this is usually achieved by invoking well known images of surveillance such as Big Brother, or by emphasizing the surveillance capacities of new technology, which implies that current changes all hinge decisively on microelectronics. In this sense, one has the impression from the popular press that some kind of technological determinism is at work, something I have argued against earlier in the dissertation. Nevertheless, the high tech paranoia popular in many media accounts has helped to draw attention to the rise of various surveillance systems in contemporary advanced societies.

On the other hand, the social benefits which accrue from many modern surveillance systems are promoted heavily in the media. These systems, it is argued, permit easy access to desirable resources. Consuming is paraded in the media as a matter of personal choice. Freedom to select between alternatives is touted as the acme of the unconstrained

life. Temporary scares over privacy may surface from time to time, but these are usually mere blips in a smoothly running megamachine that constantly gathers, stores, matches, processes, and sells personal data.

It is no wonder, then, that privacy activists generally have been unable to use the media to increase public awareness about privacy. While there is potential to educate the public, through the media, about how electronic technologies facilitate a massive augmentation of surveillance capacity in contemporary societies, consumer surveillance also depends on those same media for its survival. This surveillance, as I suggested in Chapter Three and in the last section, is usually not direct or coercive, but nonetheless succeeds spectacularly in teaching consumer skills, and encouraging consumers to internalize marketplace rules of behaviour. In this regard, Kevin Wilson argues that social responses to corporate initiatives are engineered by creating and manipulating needs that have never been a subject of public debate (1988). Social management, for Wilson, thus threatens democratic polity by exacerbating inequalities of knowledge, and making consumers more and more vulnerable to corporate power ("information rich" versus "information poor" consumers).

All of this sharpens the question of whether the contradictory relationship that exists between privacy activists and the media can be changed in a way that would pose any real challenges to surveillance. During the debates in Quebec on Bill 68, for instance, certain members of the Quebec media became strong voices for privacy protection, including Michel Venne of *Le Devoir* and several journalists for Radio Canada's consumer show "Tout Compte Fait", which gave a great deal of air time to privacy issues (Boyer,

1996: 7-8). The presence of these "activist" journalists can be attributed to the activist interpretation of the journalist's role in Quebec in the 1970s (Raboy, 1983 and Saint-Jean, 1993). At that time, journalists were fighting to gain control over issue definition from editors who were heavily controlled by commercial interests (Raboy, 1983 and Saint-Jean, 1993). This resulted in a major boom in Quebec news media of all kinds in the 1970s (Boyer, 1996).

Additionally, privacy activists can take credit for the development of an activist media in Quebec (Boyer, 1996: 7-8). Indeed, their strategy to feed the media with solid, reliable information ranging from reports, statistics, and comparative analyses of events as they unfolded, helped to create a kind of synergy between privacy activists and journalists. This is a development yet to be seen elsewhere in Canada (Raboy, 1983 and Saint-Jean, 1993), although we have seen that it has happened between breast cancer activists and journalists across the United States.

Even with this "synergy" though, contemporary surveillance practices remain difficult to challenge, which brings us back to the first lesson from breast cancer activists. It is difficult to involve the media in a public awareness campaign when privacy continues to be defined in the private realm. As Kress argues, to assign an event to the sphere of the private is at once to declare it void of power, and to assign responsibility to individuals. We have seen that when individuals are responsible for privacy, weak privacy or data protection policies ensue, if they are developed at all (Regan, 1995). On the other hand, if corporate or government organizations that are part of the public realm were responsible for privacy, privacy's broader social importance could be recognized. In this regard, the

media would have a crucial role, for instance, by exposing organizations that transgress fair information principles or the terms of the Canadian Standards Association's *Model Code for the Protection of Personal Information*. In this sense, the media would function as "watchdogs", reinforcing activist discourses which define privacy within the public domain, and thus beyond individual responsibility.

Bridging Two Public Awareness Movements: Breast Cancer and Privacy

Throughout the dissertation, I argue that surveillance has become a major feature of contemporary advanced societies and as such, it should be a focus of both social analysis *and* political action. This chapter has focused on the latter by demonstrating how those struggling directly with surveillance realities in the social and political arenas might benefit from the experiences of breast cancer activists. In particular, the chapter suggests that breast cancer activists in the United States have been successful in three social processes, each of which contains some important lessons for those who are concerned with increasing public awareness about surveillance: (1) the definitional reconstruction of issues; (2) pressure group organization; (3) and media use. By examining each of these social processes, the chapter has bridged two public awareness movements - breast cancer and privacy. As such, it has shown that the kinds of debates within which surveillance features are diverse, and that greater integration between these debates can only be beneficial.

This is an important idea in light of the dystopic paradigms that tend to dominate discussions of surveillance. Dystopias - like *Nineteen Eighty-Four* or the Panopticon -

mislead if taken too far within social analysis because they are unable to articulate, except by implication, what might be a desirable state of affairs rather than an undesirable one. In addition, they encourage a form of fatalism. Even if we understand dystopia as a warning about what might happen if nothing is done about it, neither *Nineteen Eighty-Four* nor the Panopticon give any clues as to what might be done. In this regard, the breast cancer awareness movement is instructive because it demonstrates that tackling the social problem of identifying hope comes down to the level of specific social processes. By examining these processes, I have demonstrated that it is possible to construct alternative models of understanding and action in the surveillance realm. Thus, I have argued that it is possible to soften scaremongering alarms about the surveillance society while simultaneously reorienting social policies and practices.

Chapter Eight: Conclusion

Conclusion

Throughout the dissertation, the argument is made that surveillance is a central feature of contemporary advanced societies and as such, it should be a major concern of both social analysis *and* political action. As such, the dissertation is divided into distinct, but overlapping, parts, with the first part focusing on social and critical theory, and the second and third parts focusing on the public policy arena. In Part I, I suggest that the history of modern societies is marked by moments at which new techniques - themselves the product of specific social circumstances - do make a decisive difference to the ways that social life is ordered (Innis, 1951). During the nineteenth and early twentieth century, for instance, the clock, in conjunction with the timetable, became a centrally significant device for co-ordinating human activities in time and space. It seems quite plausible to suggest that an analogous shift is taking place in the later twentieth century. Now the computer, merged with telecommunications, serves to articulate and co-ordinate human activities, but on a massively amplified scale compared with what clocks and timetables could achieve.

To concentrate thus on the consequences of technological development certainly does not constitute technological determinism. After all, I also indicate in Part I that it was the growth of democratic polity, plus the felt need for greater military and economic co-ordination, that gave the new technologies their chance. Rational, instrumental calculation existed long before the advent of computers, even though they now embody, express, and indeed reinforce just such processes. But it is precisely that remarkable

capacity of computers to contribute to the processes of co-ordination and control that make them so significant in the surveillance context (Robins and Webster, 1989).

As we have seen in Part I, computer power is now central to the apparatus of surveillance within the nation-state, and to monitoring and supervision in the workplace; indeed, "place" is actually less important to the computerized enterprise. Computer power is also central to commercial surveillance, seen by some as "social management". Both in specific ways, then, and also in terms of the general impact of computerization, new technology may be crucial to a "new surveillance". However, it remains an open question how far the use of information technology increases the power of organizations over the populations under surveillance. How far is social order constructed and maintained through consumer seduction and classificatory constraint by computer?

At this point, my earlier discussion of the Panopticon from Part I comes into its own. An increasingly commonplace argument is that what Bentham's Panopticon lacked by way of technological sophistication has now been realized courtesy of information technology. Making visibility a trap, subordination *via* uncertainty, rule by classification; all these may be accomplished routinely, remotely, and efficiently using computer databases. Data subjects collude with their own surveillance, whether by using credit cards, quoting numbers from their driver's licences, or by making telephone calls. The Panopticon metaphor has been effectively linked with surveillance at the state administration level and within capitalist surveillance in both workplace and consumer contexts. Some have also hinted at the emergence of a kind of societal Panopticon.

As we have seen, in fact different kinds of arguments operate here. The Panopticon metaphor is pressed into service within quite widely varying accounts. These range from the highly specific and particular - Zuboff on management practices, for instance - to the generalized. Among the former, specific institutions must be analysed. It clearly will not do simply to see the quintessentially modern Panopticon reproduced and amplified electronically, as if this form of social control necessarily persists once it is established. Among the latter, Mark Poster's analysis of what he calls the "Superpanopticon" stands out. He discusses the ways that the Panopticon, as a technology of power in Foucault's sense, has been electronically extended in the later twentieth century. Not only does this mean that the population is monitored "silently, continuously, and automatically along with the transactions of everyday life" (1989: 123) but, according to Poster, that the public/private distinction is eroded and another self is constituted for the individual which may be "as socially effective as the self that walks in the street" (1989: 123).

The difference between Poster's position and those of others who have discussed the Panopticon in an electronic context lies in his stress on the linguistic experience entailed within it. It is the electronic nature of the communication that distinguishes this surveillance from others. Poster insists that social analysis be concerned to explore these "new modes of linguistic experience in a manner that reveals the extent to which they constitute new modes of domination" (1989: 123). This of course is precisely the point of my analysis in Part I, in particular the empirical examination of three surveillance spheres - government administration, the capitalist workplace, and the consumer marketplace.

As far as the empirical study[10] is concerned, the main conclusions of Part I may be summarized as follows. First, the range of settings within which the investigation of electronic surveillance may be undertaken is enormous. I have looked, for instance, at the United States Internal Revenue Service and electronic ID cards in various countries. In the domain of the private enterprise, one might mention computer matching in various contexts; employee screening, remote monitoring of employees, the surveillance side-effects of information management using computer databases, direct mail, Caller ID systems, geodemographic market clustering, and videotex. These systems are constantly multiplying and expanding, frequently "feeding on themselves" as James Rule says (1983).

It is important to be aware of this vast range of applications of computer-based technology, simply because the computer does make such a difference. Above all, information technology enables many other processes to work and tasks to be performed. Even without going so far as to specify qualitative changes following in the wake of computers, it is essential to get a grasp of the magnitude of the alterations that these new technologies have engendered. As Jacques Ellul, whose work on the "technological society" antedated current critical concern with technology, says, "I must now rethink a good portion of my theory on the technological world because the computer is having ubiquitous consequences *unlike any other technology*" (my italics, 1981: 56).

---

[10] By using the term "empirical study", I do not for a moment intend to suggest that a wedge can be driven between this and, say, "critical theory". On the contrary, theory is ever underdetermined by so-called facts, and those facts are invariably theory-ladden. All I mean by "empirical" is "supported by observable evidence", that is, the kinds of descriptive activity undertaken in Chapter Two.

Second, in all these contexts, though more pronouncedly in some than others, surveillance capacities are expanded using information technology. In terms of the ability to store files, the comprehensivity of reach, the speed of data flow within and between systems, and the degree of subject transparency, surveillance is intensified. For James Rule, with whom the concept of surveillance capacities originated, limitations on these capacities are all that stands between us and the "total surveillance society" (1973). Today, the expansion of surveillance capacities becomes more generalized as increasing contacts are established between hitherto separate surveillance realms, making it more and more difficult to maintain earlier critical distinctions between those realms.

Third, new categories of social relationships do seem to be emerging based upon the "data image". This, by the way, is a significant aspect of the "electronic text", as noted by Poster. As computer-telecommunications systems facilitate the co-ordination and articulation of social activities in time and space, thus reducing those kinds of distance between people, other sorts of distancing may paradoxically be occurring. As far as data subjects are concerned, some trust must be vested in the abstract systems on which all rely from day to day. But this is a different kind of trust from that obtaining, typically, between people (Giddens, 1990).

Questions of trust and identity relate closely with conceptions of human dignity, as I argue in Part I in my discussion of *participation*, *personhood*, and *purposes*. But surveillance systems do not operate on these criteria, and it is not clear how anything different could be the case. It would not be surprising if trust turned rather easily to suspicion on the part of data subjects as the full significance of new surveillance systems

becomes clearer. The phenomena of computer fraud, hacking, and so on demonstrates that new technologies also present new opportunities for revenge on the "system", not to mention others, such as refusing to hold credit cards, for avoiding it. This fear of the instrumental gaze without moral discernment is the whole story of "distancing". Distancing can also be seen as a boon to those used to discrimination on the basis of skin colour, gender, or disability. Software can be structured precisely to minimize prejudice (Lyon, 1990). The dialectic of control, it seems, is only thinly or temporarily veiled.

Fourth, the evidence from different social spheres has made it increasingly clear that, whether or not new surveillance technologies have consequences of their own, they help to reproduce and reinforce existing social divisions. Whether in social welfare administration, the workplace or the marketplace, cleavages between labour and capital or, perhaps even more significantly, between consumers and non-consumers, do not appear to be healed by virtue of new surveillance processes. On the contrary, panopticon classification devices, along with the categorization of populations for inclusionary order or exclusionary control, are encouraged and facilitated by information technology.

Thus, to speak of a "new surveillance" or to discuss the dimensions of the emerging "surveillance society" is not hyperbole. The range and depth of quantitative changes alone would be sufficient to warrant the use of such language, without ever relapsing into technological determinism. However, much of the evidence presented in the dissertation also hints strongly that the possibility of qualitative changes should not be easily discounted. The rise of surveillance networks that are integrated across the conventional boundaries of polity and economy, the idea that a new disorganized - that is,

less hierarchically systematic - surveillance is visible in the workplace, the novel ways that consumer surveillance crosses the domestic threshold, and the pervasive importance of electronic language, seen above all in the data image, all testify to the emergence of apparently unprecedented social arrangements within the surveillance rubric.

So much for the social analysis of new technologies, their origins, and their consequences. What of the actual experience of this new surveillance by its subjects? In the second and third parts of the dissertation, I note that fears about "Big Brother", concerns about democracy, and worries about personal dignity have given rise to resistance, albeit of a limited and muted kind. This resistance has been expressed in a number of ways over the past few decades of electronic surveillance expansion.

In Part II, I focus on *technical* challenges to electronic surveillance, expressed through privacy codes of practice and privacy law in particular. In this regard, I examine four background conditions and three proximate events for policy reform at the federal level. These background conditions are: the market implications of inconsistent privacy standards in Canada; the effect of emerging data protection rules within the international arena; strong and growing privacy concerns as expressed through Canadian public opinion surveys; and the erosion of the boundaries between the public and private sectors as a result of shifting organizational functions in response to new technologies. The proximate events described in Part II are: the *Model Code for the Protection of Personal Information* developed by the Canadian Standards Association (CSA); the final report of the Information Highway Advisory Council (IHAC) which recommended the development of a "flexible legislative framework for both public and private sectors"; and the *Private*

Sector Protection of Personal Information Act drafted by the Uniform Law Conference of Canada (ULCC). By describing these conditions and events, I give some guidance to the future framework for privacy protection policy in Canada. That is, I suggest key features of the emerging "Canadian model" for personal data protection in the private sector.

From a critical point of view, the privacy laws (both current and future) analysed in Part II may be located within what might be called "postindustrial society theory". In this perspective, technological change is vitally bound up with the future progress of the advanced societies. Difficulties this progress presents may be countered, according to this perspective, not by structural modifications, but by piecemeal improvements. Does data collection threaten privacy? Technical and legal solutions may be sought with which to neutralize such threats. Indeed, the very appearance of political strife becomes less likely as technical decisions become predominant.

This is not intended as a cynical commentary on privacy legislation. On the contrary, I insist in Part II that privacy law is tremendously important, not least because it institutionalizes in law the idea that surveillance should not be permitted to grow unimpeded. However, it would be dishonest to conceal my view, which is also evident in Part II, that what can be achieved by means of legal measures is chronically limited, not only in the sense that such measures may be "too little, too late", but also in the sense that the law itself is inadequate to the task of regulating electronic surveillance. Social, cultural, and political approaches, though less tangible, may be more appropriate.

This brings me to the final part of the dissertation, in which I analyse ***mobilization*** challenges to surveillance. Mobilization challenges differ from technical responses in that

they attempt more radical questioning and opposition to the perceived negative consequences of surveillance practices, although their key aims often include pressure for the adoption of legal limits. They relate to social movements (Melucci), and the number committed to what might be called "counter-surveillance" may be growing, often spurred by technological developments such as Caller ID, smart cards, and national identification systems. Some may turn out to be short-lived, specific mobilizations to counter some blatant offence against public opinion, others more permanent manifestations of resistance.

If technical responses to the challenge of surveillance may be thought of in terms of postindustrial society theory, then mobilization responses relate to some kind of critical theory of postmodernity, particularly in their relation to social participation and the "good society". Postmodernity refers to a debate about a social transformation supposedly taking place towards the end of this century, in which we move beyond the modern condition. However, present surveillance theory is dominated by models and metaphors deriving from the modern era. The discourse of Big Brother demonstrates this most clearly; Orwell's prescience was limited, for example, to state power and primitive technology, and left a legacy of pessimism. Globalization and the subtle sophistication of information technology were not anticipated by him. Similarly, the case of the Panopticon, whose relevance to postmodern analysis is currently being explored to advantage, engenders fear at best and paranoia at worst.

But paranoia will not do as a response to contemporary surveillance because it is blind to the subtleties of surveillance which, I have shown, enables and empowers as well as constrains and limits action. Furthermore, paranoia produces political paralysis, as

noted in Part III. Either a form of fatalism takes over, or else energies are spent protecting privacy as a sphere of privilege. As an alternative, I propose in Parts I and III that some clear conception of elements of a "good society" be articulated with the analysis of surveillance, so that constructively critical theory can be made available. My understanding of the present situation has convinced me that notions akin to *participation*, *personhood*, and *purposes* would serve well. Preoccupation with pessimistic prognoses or with privacy could be sidestepped and genuine progress made towards appropriate responses. But their virtue is not merely to be analytical, as if that occurred in a moral and political vacuum. The concepts of *participation*, *personhood*, and *purposes* could also serve to reorient policy and practice, as I have demonstrated in the case of breast cancer activism. In this regard, I have shown how these concepts have found an important role within three social processes: definitional reconstruction of issues; pressure group organization; and media use. This has resulted in higher visibility, organizational strength, and permanence for the breast cancer awareness movement. Thus, I have shown through a case study on breast cancer activism how privacy activists may create space for alternative models of understanding and action, in spite of the fact that the major analytical approaches in surveillance studies are tied to modern paradigms which continually emphasize fearful futures.

Finally, this dissertation demonstrates that the construction of alternative models of understanding and action is important not only if we are to eschew fatalism or paranoia, but also if we are to face the future with realism and hope. Today, surveillance reaches well beyond the requirements of the nation-state and the capitalist workplace to the realm

of consumption and the household. In addition, surveillance has been amplified in the late twentieth century by electronic technologies which serve as a potential mode of domination, disciplining us, however subtly, to adjust to the prevailing norms of consumer citizenship. Contemporary surveillance must be understood in light of these changed circumstances. As such, this dissertation has sketched a vision that catches some elements of hope, coupled with the realism of historical and sociological analysis. In so doing, it supports a fundamental argument of the dissertation - that if we recognize that surveillance is a central institutional area of contemporary societies calling for both forms of social analysis *and* political action, we may be capable of transforming our present situations into something different and desirable. We may not see these "new" situations yet, but they are not too much to hope for.

Appendix One

Organizations and Agencies that have Provided Information for Chapter Four

Trade Associations:

Associated Credit Bureaus of Canada

Cable TV Standards Foundation

Canadian Bankers Association

Canadian Direct Marketing Association

Canadian Life and Health Insurance Association

Information Technology Association of Canada

Insurance Bureau of Canada

Stentor Telecom Policy Inc.

Individual Companies:

American Express

Bell Canada

Equifax

Consumer and Labour Organizations:

Canadian Labour Congress

Consumers' Association of Canada

Public Interest Advocacy Centre

Federal and Provincial Government Agencies:

Access to Information Commission in Quebec

Department of Justice

Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Ontario

Others:

Canadian Association of Better Business Bureaus

Canadian Information Processing Society

Quality Management Institute

Standards Council of Canada

Appendix Two

Organizations and Agencies that have Provided Information for Chapter Seven

National and Regional Organizations:

Breast Cancer Action (USA)

California Breast Cancer Organizations

National Alliance of Breast Cancer Organizations (USA)

National Breast Cancer Coalition (USA)

Save Ourselves (USA)

Individual Companies:

Avon

Revlon

Federal Government Agencies:

National Cancer Institute (USA)

National Institutes of Health (USA)

Office of Research on Women's Health (USA)

References

Abercrombie, Nicholas et al. *Sovereign Individuals of Capitalism*. London and Boston: Routledge, 1986.

Allen, Anita. *Uneasy Access: Privacy for Women in a Free Society*, Totowa, New Jersey: Rowman and Littlefield, 1988.

Altman, Roberta. *The Politics of Breast Cancer: Waking Up, Fighting Back*, Boston: Little, Brown and Company, 1996.

Akay Information Consulting Inc. *Privacy and the Canadian Information Highway: Review of Comments Received on the Industry Canada Discussion Paper*, Carleton Place, Ontario: Akay Information, 1995.

Armitage, K.J., L.J. Schneiderman, and R.A. Bass. "Response of Physicians to Medical Complaints in Men and Women," *Journal of the American Medical Association*, 5 (18), 1979, pp. 6-33.

Bauman, Zygmunt. *Modernity and Ambivalence*, Cambridge, UK: Polity Press, 1992.

Bennett, Colin. "The Formation of a Canadian Privacy Policy: the Art and Craft of Lesson-Drawing," *Canadian Public Administration*, 33, 1990, pp. 551-70.

----- "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy in the 1990s," *Science, Technology and Human Values*, 16, Winter, 1991, pp. 51-69.

----- *Regulating Privacy Codes of Practice: A Report to the Canadian Standards Association*, Rexdale, Ontario: CSA, PLUS 8830, 1995.

----- "The Politics and Policy of Data Protection: Experiences, Lessons, and Perspectives," *International Review of Administrative Sciences*, 62 (4), December 1996, pp. 459-64.

----- "Rules of the Road and Level-Playing Fields: the Politics of Data Protection in Canada's Private Sector," *International Review of Administrative Sciences* 62 (4), December, 1996, pp. 479-92.

----- *Regulating Privacy in Canada: An Analysis of Enforcement and Oversight in the Private Sector*, Ottawa: Industry Canada, 1996.

----- "Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada", *International Review of Law, Computers and Technology*, 11 (1), 1997, pp. 79-92.

Bentham, Jeremy. *Jeremy Bentham: Collected Works*, in J. Bowring (ed)., London, 1843.

Boyer, Nicole-Anne. "The Road to Legislation Part 1: The Story Behind Quebec's Bill 68," *Privacy Files*, 1 (5), March 1996, pp. 7-8.

Braverman, Harry. *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*, London: Monthly Review Press, 1974.

"British Dmers are Worried over European Data Board," *DM News*, March 5, 1990, pp. 1, 26.

Brown, Geoffrey. *The Information Game: Ethical Issues in a Microchip World*, London and New York: Humanities Press, 1990.

Canadian Bankers Association (CBA). *Model Privacy Code for Individual Customers*, Toronto: CBA, 1990.

Canadian Direct Marketing Association (CDMA). *Privacy Code*, Don Mills, Ontario: CDMA, 1993.

Canadian Life and Health Insurance Association (CLHIA). *Right to Privacy Guidelines*, Toronto: CLHIA, 1993.

Canadian Standards Association (CSA). *Model Code for the Protection of Personal Information*, CAN/CA-Q830-96. Rexdale, Ontario: CSA, 1996.

Canadian Television Standards Council (CTSC). *Cable Television Customer Service Standards*, Ottawa: CTSC, 1991.

Castells, Manuel. *The Information City: Information Technology, Economic Restructuring and the Urban-Regional Process*, New York: Basil Blackwell, 1989.

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

Chambliss, Lauren. "The Cost of Breast Cancer," *Working Woman*, October 1994.

Clarke, Roger. "Just another piece of plastic for your wallet," *Prometheus*, 5 (1), 1987, pp. 22-45.

----- "The Digital Persona and Its Application to Data Surveillance," *Information Society*, 10, 1994.

Cohen, Stanley. *Visions of Social Control*, Cambridge, UK: Polity Press, 1985.

Crimmons, J. "Bentham on Religion: Atheism and the Secular Society." *Journal of the History of Ideas*, 47, 1986, pp. 95-110.

Dandeker, Christopher. *Surveillance Power and Modernity*, Cambridge, UK: Polity Press, 1990.

Davies, Simon. *Monitor: Extinguishing Privacy on the Information Superhighway*, Pan Books, 1996.

de Tocqueville, Alexis. *Democracy in America*, Glasgow: Collins, 1968.

Decew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, New York: Cornell University Press, 1997.

Dekong, Karen. "Environmental Deregulation - A Recipe for Cancer," *World Conference on Breast Cancer*, Kingston, Ontario, July 13-17, 1997.

Dresser, Rebecca. *The Hastings Center Report*, January/February, 1992.

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

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

Flaherty, David. *Protecting Privacy in Two-Way Electronic Services*, White Plains, NY: Knowledge Industry Services, 1985.

Fortner, Robert. "Physics and Metaphysics in an Information Age," *Communication*, (9), 1986, pp. 151-72.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, New York: Vintage, 1977.

----- In C. Gordon (ed)., *Power/Knowledge*, Brighton, UK: Harvester/ New York: Pantheon, 1980.

Gandy, Oscar. *The Panoptic Sort: Towards a Political Economy of Personal Information*, Boulder, Colorado: Westview Press, 1993.

Gavison, Ruth. "Feminism and the Public/Private Distinction," *Stanford Law Review*, 45 (1), 1992.

Giddens, Anthony. *The Nation-State and Violence*, Cambridge, U.K.: Polity Press, 1985.

----- *Social Theory and Modern Sociology*. Cambridge, UK: Polity Press, 1987.

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

Gordon, Diana. "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System," *Politics and Society*, 15, 1987, pp. 483-511.

Graham, Peter. "The Australia Card," *The Australian Quarterly*, Autumn, 1987, pp. 4-14.

Habermas, Jurgen. *Legitimation Crisis*, London: Heinemann, 1976.

Hencke, David. "Big Brother Everywhere," *The Guardian*, January 16, 1987, p. 1.

Himmelfarb, Gertrude. *Victorian Minds*, New York: Knopf, 1968.

Hodgett, J.E. "The Civil Service when Kingston was Capital of Canada," *Historic Kingston*, 5, 1956.

Holvast, Jan. "Vulnerability of Information Systems," in *Managing Information Technology's Organizationsal Impact*, R. Clarke and J. Cameron (eds)., North Holland, 1991.

Industry Canada. *Privacy and the Canadian Information Highway*, Ottawa: Industry Canada, 1994.

----- *Building the Information Society: Moving Canada into the 21st Century*, Ottawa: Industry Canada, 1996. [http://info.ic.gc.ca/info-highway/ih.html]

Information Highway Advisory Council (IHAC), *Connection, Community, Content: The Challenge of the Information Highway*, Ottawa: Minister of Supply and Services Canada, 1995.

Innis, Harold Adams. *The Bias of Communication*, Toronto: University of Toronto Press, 1951.

Jay, M. ""In the Empire of the Gaze: Foucault and the Denigration of Vision in Twentieth Century Thought," in L. Appignanesi (ed)., *Postmodernism: ICA Documents*, London: Free Association Books, 1989.

Kahane, Deborah Hobler. *No Less a Woman: Ten Women Shatter the Myth abut Breast Cancer*, New York: Simon and Schuster, 1993.

Kress, Gunther. "Language in the Media: The Construction of the Domains of Public and Private," *Media, Culture and Society*, 8, 1986, pp. 395-419.

Kushner, Rose. *Alternatives: New Developments in the War on Breast Cancer*, Cambridge, Massachusetts: Kensington Press, 1984.

Kling, Rob and Jonathon Allen. "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy," in Lyon, David and Elia Zureik (eds)., *Computers, Surveillance and Privacy*, Minneapolis: University of Minnesota Press, 1996, pp. 104-31.

Lash, Scott and John Urry. *The End of Organized Capitalism*, Cambridge, UK: Polity Press, 1987.

Laudon, Kenneth. *The Dossier Society: Value Choices in Design of National Information Systems*, New York: Columbia University Press, 1986.

Lawson, Ian. *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector*, Ottawa: Public Interest Advocacy Centre, 1992.

----- *Privacy and the Information Highway: Regulatory Options for Canada*, Ottawa: Industry Canada, 1995.

Long, Murray. "First Efforts To Draft Privacy Law Seen as Lacking by Many Parties," *Privacy Files* 2 (4), 1997, pp. 8-9.

Louis Harris and Associates. *The Commonwealth Fund Survey of Women's Health*, July 14, 1993.

Love, Susan, M.. M.D. *Dr. Susan Love's Breast Book*, Reading, Mass: Addison-Wesley, 1990.

Lynn, Helen. "Mapping for Empowerment: Links between Breast Cancer Incidence and Environmental Pollution," *World Conference on Breast Cancer*, Kingston, Ontario, July 13-17, 1997.

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

----- "The New Surveillance? Electronic Technologies and the Maximum Security Society," *Crime, Law and Social Change* 17, 1992.

----- "Surveillance Societies, Privacy, and Social Control: Trends and Counter-Trends," *Crime, Law, and Social Change*, 17, 1992.

Lyotard, Jean-Francois. *The Postmodern Condition*, Manchester: University of Manchester Press/Minneapolis: University of Minnesota Press, 1984.

MacKinnon, Catherine. *Towards a Feminist Theory of the State*, Cambridge: Harvard University Press, 1989.

Marshall, T.H. *Citizenship and Social Class*, London and New York: Cambridge University Press, 1950.

Marx, Gary. "The Iron Fist in the Velvet Glove: Totalitarian Potentials within Democratic Structures," in J.F. Short (ed)., *The Social Fabric*, Beverly Hills, CA: Sage Publications, 1986.

----- *Undercover: Police Surveillance in America*, Berkeley, CA: University of California Press, 1988.

Marx, Karl. *Capital, Volume One*, Harmondsworth: Penguin, 1976.

Mazur, Allan. "U.S. Trends in Feminine Beauty and Overadaptation," *Journal of Sex Research*, August 1986.

McInnes, D. "Can Self-Regulation Succeed?", *Canadian Banker*, March/April, 1996.

Meadow, R.C. (ed)., *New Communications Technologies in Politics*, Washington, DC: Washington Program of the Annenberg School of Communications, 1985.

Melody, William. *Some Characteristics of Knowledge in an Information Society*, London: Canada House Lectures No. 31, 1986.

Melucci, Alberto. *Nomads of the Present*, London: Hutchinson Radius, 1989.

Menzies, Heather. *Whose Brave New World: The Information Highway and the New Economy*, Toronto: Between the Lines, 1996.

Merkatz, Ruth, Grant Bagley, and Jane McCarthy. "A Qualitative Analysis of Self-Reported Experiences Among Women Encountering Difficulties with Silicone Breast Implants," *Journal of Women's Health*, 2 (2), 1993, pp. 20-46.

Monroe, Linda Roach. "Let Us Heal Ourselves, Women Scientists Say," *Miami Herald*, July 18, 1993, p. D15.

Moore, John. "They Want You to be a Junk Mail Junkie," *The Independent*, London, 16 October 1990, p. 25.

Mosco, Vincent. *The Pay-Per Society: Computers and Communications in the Information Age*, Toronto: Garamond, 1989.

National Institutes of Health Guide to Grants and Contracts, NIH, August, 1993.

"National Institutes of Health: Problems in Implementing Policy on Women in Study Populations," General Accounting Office, June 18, 1990, pp. 1-106.

Nichols, Mark. "Women's Health: New Attitudes, New Solutions," *Maclean's*, 111 (2), January 12, 1998, pp. 52-63.

Olsen, Frances. "The Myth of State Intervention in the Family," *University of Michigan Journal of Law Reform*, 18 (835), 1985.

Ontario Information and Privacy Commissioner and Netherlands Registratiekammer. *Privacy-enhancing Technologies: the Path to Anonymity*, Toronto: OPIC, 1995.

Orwell, George. *Nineteen Eighty-Four*, Harmondsworth: Penguin, 1954.

Osimo, Cheryl. "The Massachusetts Breast Cancer Coalition: Activism, Advocacy, and Science from an Activist's Perspective," *World Conference on Breast Cancer*, Kingston, Ontario, July 13-17, 1997.

Panter, Audrey. "Breast Cancer as an Environmental Health Issue: Structural Impacts and Social Responses," *World Conference on Breast Cancer*, Kingston, Ontario, July 13-17,1997.

Pateman, Carole. "Feminist Critiques of the Public/Private Dichotomy," in *The Disorder of Women: Democracy, Feminism, and Political Theory*, Stanford: Stanford University Press, 1989.

Peladeau, Pierrot (1996) "A 'Model Act' in the Making", *Privacy Files* 2 (1), pp. 2, 12.

Poster, Mark. *Critical Theory and Poststructuralism: In Search of a Context*, Ithaca, New York: Cornell University Press, 1989.

----- *The Mode of Information*, Cambridge, U.K.: Polity Press, 1990.

Public Interest Advocacy Centre (PIAC), *Surveying Boundaries: Canadians and their Personal Information*, Ottawa: PIAC, 1995.

Raab, Charles and Colin Bennett. "The Politics and Policy of Data Protection: Concluding Observations," *International Review of Administrative Sciences*, 62, December 1996, pp. 569-74.

Raboy, Marc. *Libérer La Communication: Médias et Mouvements Sociaux au Quebec, 1960-1980*, Nouvelle Optique, 1983.

Rankin, Murray. "Privacy and Technology: A Canadian Perspective," in Science Council of Canada, *A Workshop on Information Technologies and Personal Privacy in Canada*, Ottawa: Minister of Supply and Services, 1985.

Regan, Priscilla. *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill and London: University of North Carolina Press, 1995.

Reichman, Nancy. "Computer Matching: Towards Computerized Systems of Regulation," *Law and Policy*, October, 1987, pp. 387-415.

Robins, Kevin and Frank Webster. *Information Technology: A Luddite Analysis*, Norwood, New Jersey: Ablex, 1986.

----- "Information as Capital: A Critique of Daniel Bell," in J. Slack and F. Feges (eds), *The Ideology of the Information Age*, Norwood, New Jersey, 1987.

----- "Plan and Control: Towards a Cultural History of the Information Society," *Theory and Society*, 18, 1989, pp. 323-51.

Rubin, Michael. *Private Rights, Public Wrongs*, Norwood, NJ: Ablex, 1988.

Rule, James. *Private Lives, Public Surveillance*, London: Allen-Lane, 1973.

----- "My mailbox is mine," *The Wall Street Journal*, August 15, 1990, p. A8.

Rule, J. and P. Attewell. "What Do Computers Do?" *Social Problems*, 36 (3), pp. 225-40, 1989.

Sabatier, Paul. "An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning Therein," *Policy Sciences*, 21, 1988, pp. 129-68.

Saint-Jean, Armande. "L'évolution de l'éthique journalistique au Quebec 1960-1990," Doctoral Dissertation, Graduate Program in Communications, McGill University, Spring, 1993.

Schuster, Neil. "ETTM Technology: Current Success and Future Potential," in *Proceedings of the IVHS America 1994 Annual Meeting*.

Shearing, Clifford and Philip Stenning. "From the Panopticon to Disneyworld: The Development of Discipline," in E. Doob and E.L. Greenspan (eds)., *Perspectives in Criminal Law*, Aurora: Canada Law Books, 1985.

Simeon, Richard. "Studying Public Policy." *Canadian Journal of Political Science*, 9, 1976, pp.548-80.

Simitis, Spiros (1996) "The EU Directive on Data Protection and the Globalization of the Processing of Personal Data," address to the "Visions for Privacy Conference," Victoria, BC, May 11, 1996.

Simmel, George. *Sociology*, Glencoe, Illinois: Free Press, 1950.

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

Snedeker, Suzanne. "Pesticides and Breast Cancer: Evaluating and Translating the Scientific Evidence," *World Conference on Breast Cancer*, Kingston, Ontario, July 13-17, 1997.

Stabiner, Karen. *To Dance with the Devil: The New War on Breast Cancer*, New York: Delacorte Press, 1997.

Stentor. *Model Code for Fair Information Practices*, Ottawa: Stentor Telecom Policy Inc., 1992.

----- *Privacy and the Information Highway: Stentor Submission to the Information Highway Advisory Council*, Ottawa: Stentor Telecom Policy Inc., 1994.

Stevens, Carol. "How Women Get Bad Medicine." *Washingtonian*, June 1995, pp. 5, 12.

Stix, Gary. "Call and Tell," *Scientific American*, April, 1991, pp. 152-3.

Strub, H. "The Theory of Panoptical Control," *The Journal of the History of the Behavioral Sciences*, 25, 1989, pp. 40-59.

Thompson, E.P. "Time, Work-Discipline, and Industrial Capitalism," *Past and Present*, 38, 1967.

Todd, James. "Better Late than Never," *Good Housekeeping*, March 1993, pp.68-70, 96.

Touraine, Alain. *Social Research*, 52 (4), 1989, p. 763.

Weber, Max. *The Theory of Social and Economic Organization*, New York: Free Press, 1964.

----- *Economy and Society*, Berkeley, University of California Press, 1978.

Webster, Frank. *Theories of the Information Society*, London: Routledge, 1993.

Weiss, M.J. *The Clustering of America*, New York: Harper and Row, 1988.

Westin, Alan. "Managing Consumer Privacy Issues - A Checklist," *Transnational Data and Communications Report*, July/August 1991.

Wilson, Kevin. *Technologies of Control: The New Interactive Media for the Home*, Madison, Wisconsin: University of Wisconsin Press, 1988.

Winner, Langdon. "A Victory for Computer Populism," *Technology Review*, May/June 1993, p. 66.

Wolf, Naomi. *The Beauty Myth*, New York: Doubleday, 1991.

Zuboff, Shoshana. *In the Age of the Smart Machine*, New York: Basic Books, 1988.