Privacy in the Political System:

Perspectives from Political Science and Economics

By

Colin J. Bennett
Department of Political Science
University of Victoria, Victoria, BC, Canada
cjb@uvic.ca

A report written for the Ethical, Legal and Social Issues (ELSI) component of the Human Genome Project, U.S. Department of Energy (coordinated by Alan F. Westin) (1995, revised 2001)

Contents

INTRODUCTION

When I first developed an interest in the privacy issue nearly twenty years ago as a graduate student, there were very few individuals with any expertise or interest in the subject. How to protect privacy was debated by a quite narrow group of experts from different countries. With only a few exceptions, privacy rarely appeared on the front pages, excited the passions of elected officials, or reached the agendas of the corporate boardrooms. All this has changed. Privacy now seems always in the news. It is debated by US Presidential candidates, and is the subject of countless legislative hearings, in the United States and overseas. Insensitivity to privacy concerns can threaten the careers of government Ministers, and damage the reputations and stock values of major companies. It appears as a major trade issue on the agendas of many international bodies. Privacy is definitely "an issue whose time has come."

Furthermore, privacy protection now has all the characteristics of an important "policy sector" of comparable importance to environmental protection. A body of statutory law (privacy and data protection legislation) now exists in most advanced industrial states, and is overseen by a network of privacy or data protection agencies that have become increasingly institutionalized at the international level. A substantial body of common law supplements these statutory rules in different countries. An international policy community of legal experts, computer and IT specialists, business and trade association representatives and public interests groups joins the governmental data protection officials for regular conferences and meetings. Privacy journals and newsletters keep this community informed of policy and technological developments. There is a large, and growing, "issue network" the participants of which have invested time and resources in becoming expert in this complex and dynamic issue.

If there is now a "politics of privacy," then it should follow that the discipline of political science should be able to add some important insights into questions about how privacy is treated within the political arena as public policy. This chapter analyses privacy from a broad perspective of *political economy* to denote the inseparability of political and economic questions. It reviews how a wide range of literature can illuminate central political and economic questions confronting advanced industrial states relating to the collection, processing and dissemination of personal information.

PRIVACY, PUBLIC POLICY, AND POLITICAL SCIENCE

Privacy and Political Analysis

There is no tradition of studying privacy within the academic disciplines of political science or economics, and therefore no identifiable tradition or cumulative literature upon which to draw. (This paper will attempt to explain this shortcoming in its conclusion.) A cursory review of the way that privacy arises in the standard political science texts and journals suggests that when the concept does appear, it is used to designate policy issues that tend to be peripheral to the major concerns of contemporary "privacy scholars." The index of the bibliographic source ABC Pol Sci lists on average ten articles per year on "privacy." An analysis of these works reveals, however, that the majority are in law journals and are related to a diversity of issues: abortion, homosexuality, the private lives of public figures, private

diplomacy, the "private" roles of women, privatization, employment law, and so on. In the International Political Science Abstracts, only one article was found with “privacy” in the title between 1989 and 2000. There are even fewer articles in standard economics journals. In one of the standard Economics reference tools (Econ Lit), no articles were found on either privacy or personal information during the same years. In neither discipline is privacy treated as a distinct area of public policy that requires political or economic analysis of its conceptualization, formation, and implementation.

Furthermore, very little has been written by political scientists or economists about "informational" (as opposed to "behavioral") privacy. The former, defined originally by Westin (1967: 7) as the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others," serves generally to restrict the analysis to the policy problem that has been created by the emergence of modern information and communication technologies. This analysis will also focus chiefly on information privacy; it is not generally concerned with the privacy literature associated with the application of the right of privacy to intimate personal decisions about abortion or contraception (e.g. Inness, 1992), or to forms of sexual behavior (e.g. Samar, 1991), or to the protection of the private lives of public figures (Warren & Brandeis, 1890). The issues do, however, intersect, as many "behavioral" privacy issues (e.g. videosurveillance, polygraph testing, intelligent vehicle highway systems, genetic testing and so on) tend to become defined as information privacy questions. In all circumstances, personal information is collected or inferred as a result of the observation of personal activity or behavior. The subsequent storage, use, and communication of that information raise a perennial set of information privacy claims.

Hence, it is impossible to confine this analysis to the literature offered by professional political scientists or economists. Our understanding of the privacy issue has been only marginally influenced by the questions that most political scientists or economists would find interesting, and by the approaches that are typically used in these disciplines to analyze other pressing policy problems. Moreover, research findings about privacy have not been seen as furthering theoretical developments within these disciplines. Thus, our discussion has to be organized not around identifiable traditions within a political science or economics literature, but according to some central theoretical questions that political and economic theorizing can and should address. This analysis covers the politics and economics of privacy, in an effort to capture the broad range of empirical and theoretical questions that are raised for both democracy and capitalism. When approached in this light, we find a wide variety of relevant materials offered by scholars affiliated with other academic departments (such as sociology, law, and business studies) as well as by journalists and others writing in a more popular vein.

Definitions of Privacy

Almost by custom, any analysis of privacy begins with a disclaimer about the inherent difficulty, perhaps impossibility, of defining "privacy" and of separating its various dimensions. Many attempts to accomplish this task have been made; and those efforts still

continue (e.g. Powers, 1994; Regan, 1995: 24-33; Lyon & Zureik, 1996: 13-17; Agre & Rotenberg, 1997: 193-95; Brin, 1998: 1). For the purposes of this review, however, it would be misleading and confining even to try to provide a general definition of "privacy" in order to focus the analysis. All definitions are, to some extent, based on questionable assumptions about individualism, and about the distinction between the realms of civil society and the state. Many gloss over essential cultural, class-related, or gender differences. Those are the very assumptions that require careful interrogation if the "politics" of privacy are to be unearthed.

Successful attempts have probably been made to specify the various roles that privacy may perform within modern political systems (Westin, 1967: 32-39; Flaherty, 1989: 8). A useful distinction can also be made between privacy as an intrinsic or aesthetic value, or the "restriction of personal information as an end in itself" (Rule, et al, 1980: 22), and privacy as an instrumental or "strategic" value. The aim of the latter is perhaps to ensure that the "right people use the right data for the right purposes" (Sieghart, 1976: 76). There is also, of course, a distinction between the claim to privacy and a "right of privacy" (McClosky, 1980). A further distinction has been made between conceiving of the right of privacy within intimate relationships, and the right of privacy as personal autonomy. These correlate to our understanding of the word "private" as meaning non-public, on the one hand, or, on the other hand, as signifying that which we prefer to keep hidden (Boling, 1994). Over thirty years of semantic and philosophical analysis, however, leaves this reviewer with the overwhelming sense that privacy is a deeply and essentially contested concept, whose meaning is often contingent and relative to time and place (Schoeman, 1984; Etzioni, 1999: 188, 196).

The same can be said of the word, "politics." Political scientists have struggled for years to place some conceptual boundaries around their discipline. Thus, we have been told that politics is the study of "who gets what, when, how" (Lasswell, 1950), or that it is the "authoritative allocation of values" (Easton, 1965), or that it is present whenever there is a will to conciliate, compromise, or debate (Crick, 1964). But there is really no consensus about the proper focus of the discipline; as a result, it has been said that political scientists tend to sit at "separate tables" (Almond, 1988): just as in a restaurant the participants enjoy a passing recognition of the conversations at other tables, for the most part the discussions are confined and unpenetrated by outsiders. Thus, any claim to define either politics or political economy of privacy raises more questions than it answers. We are dealing with two inherently problematic and contestable concepts.

The issue of personal privacy, as it has been framed within advanced industrial states, raises a number of fascinating political questions that overlap the disciplines of political science and economics. The starting point, therefore, is not an abstract and inevitably contestable conception of privacy, or an artificial definition of disciplinary boundaries. Rather the starting-point is the theoretical and empirical questions that have been raised about privacy, or should be, for any scholar of the politics and economics of advanced industrial states.

Questions to Be Addressed

First, what does the tradition of political theory contribute to the debate about the appropriate "balance" between privacy interests on the one hand, and wider societal and community obligations on the other? This debate raises central theoretical questions about the relationship between the individual and the state, about the boundaries of the public and the private, and about the essential contest between individual liberty and social values and concerns.

Second, what is the relationship between attitudes toward privacy and political culture and ideology? Here we raise questions typically within the realm of comparative politics. Is concern for privacy rooted in deep-seated cultural orientations towards the state, and is there any evidence of systematic variation across democratic political systems? As a political issue, is privacy a concern on the left and of the political spectrum, the right, or neither? What are the ideological underpinnings of the issue?

Third, what can political science tell us about the nature and extent of surveillance? This focuses on the qualitative and quantitative changes in the power of public and private organizations created as a result of new technology practices. What do we know about the nature and source of these trends? What can we say about their impact on individuals and society?

Fourth, what can political science (and particularly the study of bureaucratic behavior) tell us about the relationship between technology and politics? The attempt to promote greater personal privacy in an age of rapid technological development raises profound questions of interest to students of public administration and organizational theory about the extent to which similar technologies have a deterministic or convergent impact on organizational choice. This issue raises in a different form the central epistemological question about the relationship between structure and agency in politics.

Fifth, when privacy is viewed as a regulatory issue, what does the response to it tell us about the way that different states manage technological change? Privacy protection raises a range of fairly traditional questions about agenda-setting, pressure group politics, the legislative response, the choice of policy instruments and policy implementation, adjudication, and evaluation.

Sixth, how can privacy be analyzed on the basis of economics or public choice assumptions? While many regard privacy as a democratic right that the state has a duty to protect through regulatory policy, others see the privacy of personal information as an inherently individual good that should only be protected through individual property claims against organizations within the context of a market society.

We conclude with some reflections on the nature of the privacy debate. We try to explain why there are so many silences within the political science literature on these issues, and why we have had to look to others (lawyers, sociologists, journalists, etc.) for the analysis of questions that are clearly within the broad realm of political economy.

PRIVACY AND THE POLITICAL THEORY OF THE DEMOCRATIC STATE

In this section, we begin by establishing the tradition from which the contemporary theory of information privacy was derived, and present the various critiques of this position. There is a tradition reflected in contemporary "privacy literature" that can be traced to some traditional assumptions about the continued viability of a liberal political philosophy and epistemology.

The Theoretical Basis for Privacy

On an epistemological level, the debate about privacy can be regarded as a debate about boundaries: the boundary between the individual and the state, the community or some other collective concept. The notion of privacy rests on notions of difference between individuals, and between individuals and the collective. I, with my liberty, autonomy, rationality, and privacy, am assumed to know my interests, and should be allowed a sphere which I own untouched by others. This societal view has its roots in the 17th century liberal political philosophy of John Locke. It rests on a conception that the dynamic force behind social progress is rooted in individual, rather than collective, efforts. Consequently, in John Stuart Mill's words, there should be certain "self-regarding" activities of private concern, contrasted with "other-regarding" activities susceptible to community interest and regulation (Mill, 1859). By extension, in Warren and Brandeis' famous phrase, there must be a "right to be let alone" (Warren and Brandeis, 1890).

Edward Shils, a twentieth century proponent of this view of privacy, wrote in the 1950s that privacy is essential for the strength of American pluralistic democracy. It bolsters the boundaries between competing and countervailing centers of power. It also reinforces the barriers between the individual and the state and within the contours of civil society (Shils, 1956: 154-60). In a similar vein, Westin has argued that, in contrast to totalitarian regimes, "a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life...Liberal democratic theory assumes that a good life for the individual must have substantial areas of interest apart from political participation" (Westin, 1967: 24). As previously noted, Westin also addressed the specific functions that privacy plays. It promotes the freedom of association. It shields scholarship and science from unnecessary interference by government. It permits the use of a secret ballot and protects the voting process by forbidding government surveillance of a citizen's past voting record. It restrains improper police conduct such as "physical brutality, compulsory self-incrimination and unreasonable searches and seizures." It serves also to shield those institutions, such as the press, that operate to keep government accountable (Westin, 1967: 25).

More contemporary writers have also drawn upon 18th century writing to bolster their claims about privacy. Robert Hallborg, for example, traces the concept of privacy as deriving from Immanuel Kant's recognition of freedom, which necessarily belongs to every person by virtue of their humanity, and requires the state to allow individuals to make

fundamental personal decisions on their own. Others see the correlation between privacy and liberty as a function of personal autonomy and development, which is not possible to achieve unless individuals can express themselves in private (Le Bris & Knoppers, 1997: 419). And Karen Struening draws on Mill's writings to develop a concept of a right to privacy that protects sexual lifestyle choice. She argues that Mill's defense of diverse ways of life and experimentation ought to be read as encouraging individual eccentricity at the expense of accepted convention (Struening, 1996: 505-11).

The modern claim to privacy, then, rests on a notion of a boundary between the individual and other individuals, and between the individual and the state. It rests on notions of a distinction between the public and the private. It rests on the pervasive assumption that there is a civil society comprised of relatively autonomous individuals who need a modicum of privacy to make rational self-regarding choices about their lives.

Critiques of the Liberal Theory of Privacy

The critique of liberal political theory as a basis for privacy has come from at least four different directions. Some, have noted for example, a definite negative dimension to the notion of privacy as the "right to be let alone." It draws attention to why one might want to be left alone, and to the criticism that privacy rights are predominantly asserted for those who have the most to hide. Here is a quotation from an early article by H. W. Arndt: "The cult of privacy seems specifically designed as a defence mechanism for the protection of anti-social behaviour" (Arndt, 1949: 69). Arndt equated privacy with the almost pathological obsession with possessive individualism: "The cult of privacy rests on an individualist conception of society, not merely in the innocent and beneficial sense of a society in which the welfare of individuals is conceived as the end of all social organisation, but in the more specific sense of 'each for himself and the devil take the hindmost" (Arndt, 1949: 70).

A similar critique of the theory of information privacy was presented in a famous article by the law and economics theorist Richard Posner. Posner's central point was that the application of the principle of information privacy has an unfortunate corollary: it allows people to conceal personal information in order to mislead others and misrepresent their character (1978b). Others, including government institutions, "have a legitimate interest in unmasking the misrepresentation." Posner wrote: "It is no answer," he continued, "that, in Brandeis's phrase, people have 'the right to be let alone.' Few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. Why should others be asked to take their self-serving claims at face value and prevented from obtaining the information necessary to verify or disprove these claims?" (Posner, 1978a: 20).

A second line of attack has come from those who find the distinction between the public and the private inherently problematic. Joseph Bensman and Robert Lilienfeld, for instance, contend that the "private and the public are inextricably intertwined and interlaced. They cannot be treated as separate entities" (Bensman & Lilienfiled, 1979: 182). They are at the very least "complex-structured concepts" that operate on different dimensions. Stanley Benn and Gerald Gaus contend that the public/private distinction must be qualified according to whether one is analyzing the "allocation of access to information, resources etc., the

capacities in which agents enjoyed that access, and in whose interest it was used" (Benn & Gaus, 1983: 7-11).

By extension, the public/private dichotomy (and therefore much theorization about privacy) has been regarded as inherently gendered. Feminists have critiqued liberalism for reifying a distinction between a private, domestic (female) world, and a public sphere that is chiefly the preserve of men (Pateman, 1983; Allen, 1985). Anita Allen and Erin Mack critique Warren and Brandeis on these grounds, stating they "were not critical of the ways in which home life, assertions of masculine personality, and norms of female modesty contributed to women's lacking autonomous decisionmaking and meaningful forms of individual privacy." They advocated "too much of the wrong kinds of privacy--too much modesty, seclusion, reserve and compelled intimacy--and too little individual modes of personal privacy and autonomous private choice" (Allen & Mack,1990: 477).

Boling praises the work of feminists such as Pateman and Susan Moller Okin, who argue that ending state power at the gate of the family home merely reinforces patriarchy, and that whoever has *public* power determines who has power in the so-called *private* sphere. Boling points out, however, that these writers often equivocate on the desire for privacy, and she argues that we must recognize that a respect for privacy can be empowering (Boling, 1996: 4-15.) In this respect she is supported by bioethicists such as Alta Charo, Ruth Faden, Dorothy Roberts, and Karen Rothenberg, who would keep women's decisions regarding abortion and other procedures private (Allen, 1997: 36).

Thirdly, from the perspective of democratic theory, some would also contend that the liberalism of Locke and Mill, upon which the theory of information privacy rests, represents just one version of democratic theory. Carole Pateman (1970), for instance, has argued that there are two general traditions of democratic theory. One is a liberal tradition rooted in 18th century natural rights theory; the other is derived from the view that the test of a democracy is not the protection of individual or minority rights, or the degree of competition between centers of power. Rather, the test is the degree of participation, cooperation, community consciousness, and so on--values that are not necessarily promoted by asserting the "right to be let alone." Information privacy is, therefore, a precondition not of democracy per se , but of a particular form of liberal democracy. The theoretical justifications for this were provided by Locke, Madison, and Mill, rather than by Jean Jacques Rousseau.

This argument finds current reflection in the renewed interest in the communitarian theorizing of Amitai Etzioni, which has resonated with contemporary political elites of the left and the right in both Europe and America. (Etzioni, 1994). Etzioni argues that the writings of J.S. Mill, Locke and Adam Smith must be understood as advocating rolling back what were, at the time, excessively oppressive and authoritarian societal controls. He writes that the "negative consequences" of treating privacy as "sacrosanct" have been "largely ignored" by those who champion individualism (Etzioni, 1999: 194-95). Citing the benefits of encryption and "Megan's Law," and criticizing "cyberspace anarchists," he advocates a conception of privacy rooted in communitarianism (Etzioni, 1999: 96, 68). That approach recognizes that our concept of privacy is rooted in a sociohistoric context, and is not a natural right (Etzioni, 1999: 200-02). He further argues that the power of individual choice can be protected, if, paradoxically, there is less individual privacy, as societal scrutiny lessens the

need for governmental control (Etzioni, 1999: 191, 197, 212-13.)

The conceptualization of distinct private and public realms almost inevitably leads the debate to a discussion of how privacy conflicts with social or community values. It often leads to the view that privacy and social values such as internal security, social welfare, government efficiency, and so on, are necessarily antithetical. The problem here is not only that these concepts are deeply contested and ambiguous, but also that the promotion of privacy can itself be socially important.

Priscilla Regan has recognized that the liberal, Lockean tradition continues to serve as the backdrop for the discussion of privacy, but she argues that it overemphasizes individual privacy and fails to address the social importance of privacy. She maintains that privacy, in addition to being a commonly held value, is also public value and collective value, precisely because it is important to a democratic political system. (Regan, 1995: 25-26, 212-14). She writes:

> Most privacy scholars emphasize that the individual is better off if privacy exists. I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes. If privacy became less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual. Even if the individual interests in privacy became less compelling, social interests in privacy might remain.(1995, p. 221)

Paul Schwartz also describes information privacy as an important element in constituting a civil society (Schwartz, 1999). Instead of personal choice being the paradigm of information control, society normatively defines standards of privacy, which limit access to information. Because the standards are multidimensional, they impose duties of confidentiality and disclosure for the same piece of information. Schwartz builds on this to suggest a set of obligations for information privacy in cyberspace. (Schwartz, 1999: 1666, 1670-73).

A final critique emerges from those who argue from post-structuralist assumptions that the essential ontological premise about the central autonomy of the subject is misguided. "Panopticon" was a term originally used by Jeremy Bentham to describe a prison which could efficiently observe prisoners at all times through a central tower or other mechanism. The system was designed to create a state of permanent and constant visibility that would maintain discipline. Michel Foucault expanded on the concept of panopticism, theorizing that it could be applied in many areas of life, and was not limited to surveillance, but could be used when classifying people by many categories. Foucault described the link between knowledge and power, and the tendency by those in power to define and separate those deemed deviant, and create norms which are culturally reinforced (Foucault 1979; Gandy, 1993).

Mark Poster explicated Foucault's notion of the Panopticon as a new form of "everyday surveillance" and social control. In so doing, Poster explained the post

modern/post-structuralist argument as follows:

> Foucault taught us to read a new form of power by deciphering discourse/practice formations instead of intentions of a subject or instrumental actions. Such a discourse analysis when applied to the mode of information yields the uncomfortable discovery that the population participates in its own self-constitution as subjects of the normalizing gaze of the Superpanopticon. We see databases not as an invasion of privacy, as a threat to a centered individual, but as the multiplication of the individual, the constitution of an additional self, one that may be acted upon to the detriment of the "real" self without the "real" self ever being aware of what is happening. (Poster, 1990: 97-8).

Poster's analysis places the "mode of information" and especially the surveillance capacity of modern information technology at the heart of contemporary social transformations. For him, the theory and language of information privacy is irrelevant. The more profound question for the postmodern era is nothing less than "where the human self is located if fragments of personal data constantly circulate within computer systems, beyond any agent's personal control" (Lyon, 1994: 18). Poster calls for a politics of databases that emphasizes not autonomy and individual privacy, but takes into account new forms of identity formation and community in an era of cyberspace and virtual reality (Lyon & Zureik, 1996: 190-91). Other critics have also cited Foucault to contend that an individually-based privacy regime locks individuals into standardized identities and arbitrary social restraints and that liberation comes from a refusal to accept such restraints (Struening, 1996: 516).

Despite these various critiques, the privacy literature has assumed a distinction between the realms of the public business of the state and the private spheres of individual life. Though the literature is vast, it has remained relatively untroubled by deeper ontological questions about the nature of the "self" in modern on postmodern conditions or about cultural relativity or bias according to class or gender. (For a deeper examination of these issues, see the previous chapters by William Regenold and Gail Geller). To some extent, this selective focus is explained by the fact that much of the more philosophical debate about privacy has been directed toward the political and legal arena. It has been said (normally by those trained in European schools) that most American political theory is but a footnote to the Constitution. In the privacy area, there is some truth in this observation. The bulk of the more abstract and conceptual literature was prompted by the need to understand the emerging "right to privacy" that the U.S. Supreme Court has developed and applied to private decisions about intimate family concerns such as contraception and abortion. Much of the philosophy of privacy is, therefore, understandably directed toward emerging legal doctrine (e.g. Prosser, 1960; Fried, 1968; Pennock & Chapman, 1971; Parker, 1974; Gavison, 1980; Parent, 1983).

Privacy Theory and Public Policy

The pervasiveness of liberal assumptions within the literature has had a number of political and policy implications. First, it explains the continuous reference in the privacy literature to the concept of balance. However conceptualized, privacy is not an absolute

right; it must be balanced against correlative rights and obligations to the community. Richard Hixson conceptualizes "balance" as the "continuing struggle over the meaning of private and public, the jurisprudential debate over individual autonomy and collective welfare, between the person and the state, the individual and the community" (Hixson, 1987: xv-xvi). Etzioni also defines communitarianism as an approach that "holds that a good society seeks a careful balance between individual rights and social responsibilities, between liberty and the common good. . . ." (Etzioni, 1999: 5).

David Brin's recent work conceptualizes the need for balance between privacy and transparency. He asks three questions: A) Where do we want to end up? B) Who has the ultimate advantage in each situation? and C) Which situation is robust or stable? He posits regulatory regimes of transparency and secrecy, and discusses which one is more likely to reward the powerful or protect the weak, and which is more realistic. He examines the advantages of transparency and secrecy along both an accountability and plausibility matrix. He makes arguments for and against each system, concluding "Perhaps we who stand at the extremes, both strong privacy advocates and believers in transparency, underestimate how smart folks really are. Over the long haul, people may work their way toward a clear-headed mixture of our purist positions, finding pragmatic ways. . . . [to secure] an enviable curtilage for average citizens and their families (Brin, 1998: 272-77). Raab reminds us, however, that "balance" is an ambiguous term that has different implications for action depending on who is doing the 'balancing" and for what reasons (Raab, 1999).

An assumption of "balance" also underlies many of the official investigations into privacy policy. The U.S. Privacy Protection Study Commission, for instance, began its analysis by declaring that "the Commission has constantly sought to examine the balance between the legitimate, sometimes competing, interests of the individual, the record-keeping organization, and society in general" (US, PPSC, 1977: xv). The assumption about balance also underlies the doctrine of "fair information principles" (FIPs) for the appropriate collection, retention, use and disclosure of personal information, although the codification of these principles has varied over time and location. They appear either explicitly or implicitly within all national data protection laws (including those in the US and Canada that are called "Privacy" Acts). They also form the basis of international agreements, such as the 1981 Guidelines from the Organization for Economic Cooperation and Development (OECD, 1981), the 1981 Convention from the Council of Europe (CoE, 1981), and the more recent Directive on Data Protection from the European Union (Council of the EU, 1995; *see also* Regan, 1994).

I have argued elsewhere (Bennett, 1988a; 1992: 101-111) that while the codification may vary, there tend to be six essential principles: 1) openness-- the very existence of personal recordkeeping systems should be publicly known; 2) individual access and correction; 3) collection limitation --organizations should only collect and store information that is relevant to accomplish a legitimate task; 4) use limitation --data should only be used for purposes consistent with those tasks; 5) disclosure limitation --personal data should only be disclosed externally for legitimate reasons or with the consent of the individual; and 6) security--against loss, unauthorized access, destruction, use, erasure, or modification of personal data. The development of these statutory principles rests on some basic liberal

assumptions about procedural justice. We all have privacy rights and interests, it is assumed, but those concerns can only be subjectively defined. No paternalistic definitions of the privacy value appear; no attempts are made to second-guess the privacy interests of individual citizens. Implicit is a rational faith in the capacity of longstanding principles of procedural justice to counter the worst effects of new technologies.

Further work on the political theory of privacy is needed. As a common problem, which has arrived on the agendas of different democratic states at roughly the same time, it provides a fascinating opportunity to interrogate wider theories about politics in advanced industrial states. Unlike some other regulatory issues, it raises central and enduring questions about the power of the state, the respect for civil liberties, the relationship between the state and civil society, and the definition of the "subject" within conditions of modernity (or postmodernity).

PRIVACY, POLITICAL CULTURE, AND POLITICAL IDEOLOGY

We now move to a series of questions broadly within the realm of comparative politics. What can an analysis of privacy tell us about different perceptions about the role of the state historically, and comparatively?

Historical and Cultural Traditions

Although examples of systematic record-keeping by governments can be found in ancient and medieval times, the rise of this practice is most closely associated with the development and bureaucratization of the modern nation-state (Tilly ed. 1975; Dandeker, 1990). The expansion and institutionalization of state power since the 16th century brought with it the need for more complex, discriminating, and formal record-keeping systems, many containing personal information. Three types of personal records can be identified: administrative records (generated by a transaction with an agency**,** used to regulate, service, license, or prosecute specific individuals, such as applying for a grant, reporting income, applying for welfare, getting married, etc.); intelligence records (secret or closed files serving an investigative purpose, such as police files); and research or statistical records (used to produce reports on general policy, planning or other studies and not regarding specific individuals, created through census or survey research methods) (Westin & Baker, 1972: 361; US HEW, 1973). The institutionalization of personal record-keeping is a trend common throughout advanced industrial states.

In a lengthy study of privacy as an idea in Western history, Westin examined five periods in civilizations which have affected modern ideas about privacy (Westin, 1965). He looked at the Greek city-state in the 5th century B.C., the Roman Empire in the 2nd century A.D., Western Europe in the 13th century, England in the 1600's and the U.S. from 1790 to 1820. While privacy and individualism both grew in Athens, Romans had less privacy and produced relatively few creative or scientific works (Westin, 1965: 81). Christian medieval life introduced the previously unknown concept of private religious meditation in daily life, but also created the Inquisition, which probed for heretical thoughts as well as acts, making it

a ruthless instrument for surveillance and oppression (Westin, 1965: 106-07). As in the periods before, while in general the wealthy could an did enjoy more privacy than the poor, psychologically, medieval man simply did not expect to have any privacy (Westin, 1965, :125).

According to Westin, it was in Stuart England that the word "privacy" came into common use among the upper classes, and Shakespeare's characters often assert their privacy. Middle class families also lived less communally with others, than in Medieval times, but large homes still sharply limited privacy (Westin, 1965: 129-40). The master of a house kept watch over the lives of his servants, and English Protestants often zealously observed each other for signs of blasphemy (practicing Catholicism, even privately, was illegal). English law did begin to recognize a right to privacy in the home, but the growth of centralized power led to increased searches. Ecclesiastical law recognized marital privacy, but secular courts did not. There was a recognition of a separation of public and private life, but society was slow to recognize it.

The early years of the American Republic found the upper and middle class guarding their privacy in the household. Of course, rights against unreasonable searches and seizures were written into the federal Bill of Rights, and many states did the same in their constitutions (Westin, 1965: 205-06). Servants had a much greater degree of privacy than before, while slaves had none. Eavesdropping was a crime, and religious and political speech in the home were immune from prosecution, although public acts of blasphemy were actionable. American law recognized the confidentiality of conversations between lawyer and client and between spouses, and in 1828 New York enacted a law protecting doctor-patient communications (Westin, 1965: 282-83). By this era, an understanding of the value of privacy had taken root, and was respected in voting, mail, association, relationships and opinion. The powers of institutions which threatened privacy - government and private authority, had been checked in favor of a strong and open legal system (Westin, 1965: 287).

Westin went on to argue in Privacy and Freedom that different historical and political traditions among Western nations were likely to create different results in the overall balance between privacy and government. Britain exhibits a "deferential democratic balance," a combination in which there is "greater personal reserve between Englishmen, high personal privacy in home and private associations, and a faith in government that bestows major areas of privacy for government operations." West Germany exhibits an "authoritarian democratic balance" in which "respect for the privacy of person, home, office and press still gives way to the claims of official surveillance and disclosure." The United States exhibits an "egalitarian democratic balance, in which the privacy-supporting values of individualism, associational life, and civil liberty are under constant pressure from privacy-denying tendencies toward social egalitarianism, personal activism, and political fundamentalism" (Westin, 1967: 26-7).

It is interesting to hypothesize that the way the balance between privacy and community obligations and duties is struck within different democratic societies will vary according to their cultural traditions. The belief in privacy is closely related to broader attitudes about participation in public affairs and about trust in the authority of governmental agencies; these issues have attracted considerable attention from students of comparative

politics (*e.g*. Almond & Verba, 1965, 1980), as well as from more anthropological perspectives on social and cultural history (Moore, 1984; 1998). Unfortunately, we have little systematic cross-national survey evidence about attitudes to privacy with which to investigate the nature and influence of wider cultural attributes. Most of this argumentation tends, therefore, to rest on anecdotal and impressionistic evidence, such as: "the Englishman's home is his castle," and so on.

Political Culture and Comparative Attitudes Toward Privacy

There is little cross-national survey evidence, but there is some. Some of the best comparative evidence for examining the relationship between attitudes toward privacy and political culture is found in opinion polls in Canada and the United States, sponsored by Equifax Inc**.,** and conducted by the Louis Harris firm under the advice of Alan Westin (Harris-Westin, 1990; Harris-Westin, 1992a, 1992b, 1994). Traditional comparative scholarship about Canada and the United States (e.g. Lipset, 1990) has suggested a profound difference in the values of the two countries that explains significant variations in institutional and policy development. The United States is arguably founded on individualist principles, creating a greater distrust in political and administrative elites and in their established institutions. Canadians are supposed to be more communitarian in outlook, resulting in a greater deference to authority and trust in public institutions.

Hypothetically, these supposed cultural orientations might be reflected in a greater respect for privacy rights in the US than in Canada. Testing this hypothesis in the 1992 survey, Westin discovered that, indeed, distrust is highly correlated with concern for privacy in both Canada and the United States. However, "in striking contrast to the traditional wisdom that Canadians are more trustful of government and political processes ... [the survey found that] Canadians have a higher combined distrust score than do Americans" (Harris-Westin, 1992b: IX). A follow-up survey in 1994 found the same privacy dynamic at work, with "high and still rising distrust remaining the most significant explanation for still rising privacy concerns" (Harris-Westin, 1994: VI).

In comparisons with European countries, a 1999 survey revealed that Americans are much more likely to be concerned about possible misuse of personal information than are individuals in Britain or Germany (IBM-Harris: 71, 165, 249; *Privacy and American Business*, 2000), and were much more likely to assert their privacy, by, for example, refusing to give out information, or asking to have their name removed from a marketing list (IBM-Harris: 23, 85, 175, 259). Perhaps not surprisingly, however, Americans had more confidence in businesses, as compared to the British and Germans in particular, who consistently showed the least confidence in industry to protect their privacy (IBM-Harris: 12-13, 47-48, 153-55, 237-38; Westin ed., 2000).

The IBM-Harris poll showed that large majorities in Germany, Britain and the U.S. were concerned about privacy, and that more than one in five believed that they personally had had their privacy invaded by a business (IBM-Harris: 69, 164, 248; Westin, 2000). In addition, users of the Internet are consistently more privacy conscious, but also have more

confidence in online businesses than those who do not use computers (IBM-Harris: 16-17, 69-73, 96-100, 164-67, 185-87, 248-49, 269-76; Westin, 2000). This may be a reflection on the temperament of individuals who choose to use the Internet, or it may be a result of experiences online, in which case it could signal a more permanent shift in attitudes as more people use the Internet.

In a survey conducted by Alan Westin and Adams Communications in November of 1999, more than 1,000 Japanese adults were polled regarding their attitudes about privacy (Westin & Adams, 2000). Three out of four Japanese consumers were concerned about privacy, and wanted companies to adopt privacy policies. But only one in ten still would have high or complete confidence in a company that adopted privacy policies (Westin & Adams: 3). 76% of Japanese consumers were concerned about possible misuse of their personal information, which put them ahead of Germany but behind the U.K. and U.S. in this regard (Westin & Adams: 6). While 60% of Americans see personalized marketing as a good thing, 53% of Japanese do not (Westin & Adams: 20). Underlying those privacy attitudes, almost six out of ten agreed that there was a clear today trend away from community or group-enforced approaches toward more individual choice in Japanese society (Westin & Adams: 12).

To conduct more refined analysis about the relationship between privacy and other cultural variables, we obviously need a more systematic cross-national study on privacy. However, individual polls on privacy (such as Germany, Britain, and Sweden) suggest superficially that populations everywhere have high, and increasing, levels of concern. This concern seems to be driven mainly by fears of new technology and distrust that public and private institutions will use that technology with sufficient respect for individual civil liberties. The distrust may be rooted in different historical experience; but it appears to be pervasive and strong (Bennett, 1992: 37-43).

Political Culture and Privacy Policy

"Political culture" is also hypothetically an explanation for the different approaches to the implementation and enforcement of privacy law. The responses of Western societies to the privacy problem have primarily differed in the institutional oversight mechanisms established to implement and enforce the fair information principles (Burkert, 1982; Bennett, 1988b). A special issue of the *International Review of Administrative Sciences*, edited by myself, Wim B.H.J. van de Donk and Charles D. Raab gathered analyses of data protection regimes in several countries, including the United States, Canada, the United Kingdom, and the Netherlands. The analyses touched on the policy making and decision making process, implementation and evaluation. We concluded that administrative cultures, attitudes toward authority, and the overall institutional arrangement of the state are neglected variables in the analysis of the enforcement and implementation of privacy protection law (Bennett, Raab, & van de Donk, 1996: 461, 572-73).

To some extent, the absence of a data protection agency in the United States can be explained by a typical American aversion to paternalism: Americans should be able to define

their own privacy interests and take steps to protect them through the courts. Indeed, the American penchant for litigation and the consequent proliferation of case law has been defended as a unique approach to privacy, that results in a level of "protection" similar to what exists in societies that have adopted a more comprehensive and anticipatory approach to the problem (Aldrich, 1982; Plesser, 1991).

Privacy advocate Marc Rotenberg, however, does not accept this view. He argues that American privacy policy is incoherent and directionless, yielding many laws, but inadequate protection (Rotenberg, 1991). The bewildering collection of federal and state laws can only be used effectively by those with the money to pursue litigation (Smith, 1992; Flaherty, 1997). Rotenberg is unpersuaded by arguments about the need for an exceptional and distinctly American approach to the problem which would presumably differ from interventionist efforts found in Europe. There, entities such as the British Data Protection Registrar, the German Data Protection Commissioner, and the French Commission Nationale de L'Informatiqe et des Libertés (CNIL) serve to protect the individual from the recordkeeping organization. Rotenberg and others (e.g. Flaherty 1984b), do not accept the argument that such an agency would be an unnecessary and alien import, inconsistent with the American administrative system, even though support for such an agency in public opinion polls is distinctly ambivalent (Harris-Westin, 1990: 104). Others have argued that the fact that Americans tend to view privacy, as they define it, as an individual right makes it difficult to formulate a policy to protect it (Regan, 1996).

Cultural differences also inform Sonia Le Bris and Bartha Maria Knoppers' study of the concept of privacy in Belgium, France, Germany, Italy, Spain, Switzerland, the nations of Scandinavia and the province of Quebec. They found that while for many years civil law limited the right to privacy, most European countries consider privacy a subjective right, which is actionable per se and does not require proof of fault. In addition, in most European countries the civil code protects privacy, as does the Universal Declaration of Human Rights and the European Convention on Human Rights. In addition, the German Basic Law has been held to include a general personality right, "the right of a person vis-à-vis another to respect for dignity and for the development of individual personality" as long as its expression did not violate the rights of others or the constitutional order and morality (Le Bris & Knoppers, 1997: 419-27).

Notwithstanding these studies, cross-national differences or similarities in the extent of concern about privacy, or in the way that policy outcomes have been shaped, are difficult to attribute in any definitive way to variations in that amorphous concept "political culture." But, are attitudes to privacy, shaped by one's ideological orientation? Does it correlate with liberal or conservative, or left and right, perspectives?

Privacy and American Political Ideology

Concern for the protection of privacy has been incorporated into a series of studies, since the 1950s, that have sought to understand the patterns of support for civil liberties and civil rights among elites and masses. The tradition probably begins with the controversial

studies by Stouffer that claimed to demonstrate a greater respect for civil liberties among elites than among the mass public (1955). The sociological roots of "toleration" have been of subsequent interest to political scientists working within the behavioral tradition (e.g. Sullivan et al, 1982; McClosky & Brill, 1983).

It is difficult to dissociate American attitudes about rights to privacy from attitudes about the gamut of civil liberties inherent in the U.S. Bill of Rights. McClosky and Brill demonstrate the most interest in privacy issues (1983: 171-231). Employing data from the 1979 Harris-Westin privacy survey, they address a range of issues about Fourth Amendment "search and seizure" questions. Some of the findings are ambiguous. Most Americans, especially elites, are preponderantly opposed to police searches without a court order. On the other hand, Americans believe (by a two-to-one-margin) that police officers who stop a car for a traffic violation should be allowed to search the car if they suspect it contains drugs or stolen goods (1983: 185).

Similar inconsistencies are apparent in the findings about wiretapping, a practice most Americans apparently generally perceive as unfair. But they do not seem to regard eavesdropping on the activities of meetings of known criminals, or to protect the nation against "radicals," as improper, especially when it is a one with a court order. The generalization from these and other privacy-related questions is that "popular support for civil liberties tends to be greater when the norms are clear and well established and weaker or more uncertain when the norms are newly emerging, still unfamiliar to many members of the mass public, and not yet firmly fixed in the body of constitutional principles endorsed by the courts" (McClosky & Brill, 1983: 185). While there remains some support in McClosky and Brill's study that "community leaders" are more likely to show more tolerance across the range of civil liberties issues (including privacy), there is little evidence that this has much to do with political partisanship or ideology: "at every level of economic liberalism-conservatism, elites score higher on the civil liberties scale than do their demographically matched counterparts in the general public" (1983: 255).

This seems also to be true with respect to attitudes about privacy protection. In a 1990 poll conducted by Louis Harris, it was discovered that "political philosophy does not seem to be much of a factor in peoples' general concerns about privacy" (Harris-Westin, 1990: 1). The only systematic relationship seems to be that those who self-describe themselves as "moderate" or "middle-of-the-road" tend to be less concerned about privacy than those identifying as "conservatives" or "liberals" (Dutton & Meadow, 1985: 39). Support for the issue also tends to be higher among Blacks and Hispanics in the United States than among whites (Dutton & Meadow, 1985: 38). However, Hispanics and African-Americans are less likely to be critical of business practices, and are more likely to believe their rights are protected, even though Hispanics, in particular, are more likely to report that they have been the victim of an improper invasion of privacy by a business (Harris-Westin, 1998: xvii).

The privacy issue seems to be sufficiently broad to embrace the concerns of those over the range of ideological viewpoints: from the civil libertarians who want controls on overzealous law enforcement, to the conservative anti-tax group that is seeking to keep the

IRS and their equivalents in check. However, James Rule asks us to keep in mind that "no one is likely to come out against privacy. But a close look at the clamor for more of it suggests that its proponents do not all have the same thing in mind" (Rule et al, 1980: 135).

In summary, there are compelling reasons to believe that the modern issue of information privacy has developed without particular regard to distinctive cultural traditions nor to the influence of different ideological orientations. On the one hand, the technology itself exerts a powerful force for cross-national convergence. What is more, the definition of the privacy problem and the various responses (through data protection or information privacy laws) has much to do with the cross-fertilization of ideas through a transnational community of privacy experts. Lessons were drawn about how best to articulate and respond to the problem. This ultimately led to harmonization efforts by international organizations. The different national concerns for privacy obviously have their source in different historical experiences. Overall, however, it can be argued that the forces for convergence have been overwhelming, and have led to similar concerns, and somewhat similar policy responses (Bennett, 1992).

PRIVACY AND THE POLITICS OF SURVEILLANCE

Some scholars have argued that the contemporary problem confronting advanced industrial states can only be imperfectly addressed and resolved if it is defined in terms of "privacy." Rather the problem should be defined as *surveillance*, or excessive and illegitimate surveillance. "Rather late in the day," David Lyon argues (1994: 219), "sociology started to recognise surveillance as a central dimension of modernity, an institution in its own right, not reducible to capitalism, the nation-state or even bureaucracy." Our next section addresses this broad concept, and how it has been treated as a political phenomenon.

Surveillance and The State

Within political science, the analysis of surveillance initially surfaced in relation to the description and critique of authoritarian or totalitarian regimes. This critique spans the centuries, from the use of "spies" within Imperial Rome, to the systematic monitoring of citizen behavior within Stalinist and Fascist systems (Westin, 1967). To a certain degree, the contemporary interest in privacy among scholars like Edward Shils and Alan Westin was motivated by a desire to build institutional and cultural barriers against the comprehensive monitoring of private life that appeared (during the Cold War years) as a necessary condition for the continuation of totalitarian regimes.

Since that time, however, questions have been raised about the creeping and subtler forms of surveillance within liberal democratic states. Several questions have been addressed. What is the nature of contemporary surveillance using new information technologies, and to what extent is it different from the practices of the past? What explains the rise of "surveillance societies"? Is it due to an inexorable extension of Weberian bureaucratic rationality? Does it flow from the deterministic logic of technological

application? Maybe all of these. Perhaps Foucault's point about the ubiquitous and "everyday" nature of power relations, in which individuals unwittingly subscribe to their own surveillance within the "panopticon" provides the central, all-encompassing insight.

From the perspective of those interested in understanding and curtailing social control, the formulation of the privacy problem in terms of striking the right "balance" between privacy and organizational "demands" for personal information hardly addresses these wider questions. The liberal political theory that underpins the "fair information practices" places an excessive faith in procedural and individual remedies to excessive intrusions. Regardless of attitudes towards privacy in the population, privacy and data protection laws can only have a marginal impact on the development of surveillance societies; some would even contend that such laws serve to legitimize new personal information systems and thus extend social control. According to Etzioni, efforts to protect privacy, at least in the United States, often prompt the government to seek even more invasive techniques to achieve the same result (Etzioni, 1999: 213-14).

The work that is normally cited as the best critique of the theory of information privacy as articulated by Westin is The Politics of Privacy (1980) by James Rule and his colleagues. Privacy and data protection laws are all well and good, but they frame the problem in too narrow a fashion. The argument is that public policies that seek to "balance" privacy rights with organizational demands for information may produce a fairer and more efficient use and management of personal data, but they cannot control the voracious and inherent appetite of all bureaucratic institutions for more and more information on individuals. They cannot halt surveillance, in other words. The essential problem for Rule then is the inherent tendency of bureaucratic organizations (public and private) to want to collect and store more and more increasingly detailed personal information. This dynamic of complex organizations has its roots in the 18th century, and the move towards rationalization and control of resources that accompanied industrialization (Beniger, 1986). The problem increases as surveillance, advanced by technology, becomes a global phenomenon (Lyon & Zureik, 1996: 4-5). Thus the "solution" to increasing surveillance can only come from the cultivation of a looser, less discriminating and less efficient relationship between organizations and their clientele.

The arguments of Westin on the one hand, and Rule on the other, have often been posited as diametrically opposed political theories of privacy and surveillance. The distinction between the two sets of literature should not be exaggerated. The difference stems more from the starting-point. For Westin, the problem is privacy and how the institutions of a liberal society might cope with the most dangerous and intrusive threats from new technologies. For Rule (and other sociologists), the starting point is an interest in the changing impact and nature of social control and disciplinary practice (Rule, 1996). The processing of personal data by private and public institutions is, from this more critical perspective, a way to shed light upon broader social and technological forces.

The idea that advanced industrial societies are creeping inexorably toward an unacceptable level of surveillance has influenced writers from a number of disciplinary and national backgrounds. David Flaherty, a Canadian scholar of legal history, ended up calling

his comparative analysis of the operation of data protection laws in Germany, Sweden, the United States, France and Canada, Protecting Privacy in Surveillance Societies. He begins: "The central theme of this volume is that individuals in the Western world are increasingly subject to surveillance through the use of databases in the public and private sectors, and that these developments have negative implications for the quality of life in our societies and for the protection of human rights" (1989: 1).

Flaherty goes on to demonstrate how countries that have established data protection agencies (like Germany and Sweden) have a better chance of stemming the tide than do countries like the United States, whose privacy protection regimes rely solely on the individual assertion of privacy rights through the courts, and on weak oversight mechanisms. But his overall conclusion is skeptical: "How will data protection authorities look by the year 2000? There is a real chance that they will be looked back upon as a rather quaint, failed effort to cope with an overpowering technological tide rather then as a fruitful, successful exercise in promoting the coexistence of competing human and social values" (1989: 406). Echoing Rule's analysis, he suggests that "at present, data protection agencies are in many ways functioning as legitimators of new technology. For the most part, their licensing and advisory functions have not prevented the introduction of threatening new technologies, such as machine-readable identity cards or innumerable forms of enhanced data banks; they act rather as shapers of marginal changes in the operating rules for such instruments of public surveillance" (1989: 384).

In 1997, Flaherty, looking back, wrote that "this debate has been handily won by the pro-privacy side of the equation, at least in most advanced industrial societies" (Flaherty, 1997: 169). But he also concluded that, on the basis of his experience as the first Information and Privacy Commissioner for the Province of British Columbia that "the pressures for surveillance are almost irresistible for an office such as mine" (Flaherty, 1997: 170). Flaherty does not believe that, as Commissioner, he has become a legitimizer of government practices, although he acknowledges his failures. He concludes that he has even less reason now to be optimistic than he did in 1989, due to the rise of Internet and the digital economy (Flaherty, 1997: 190), despite the fact that the privacy value has survived since the advent of recorded history (Flaherty, 1999).

Surveillance and the Public

The rise of the "surveillance society" (to use Flaherty's phrase) has been traced in a wide-range of less scholarly books from a number of countries. Orwellian metaphors and imagery are naturally prolific, even though "1984" came and went without any palpable change in the attention paid to privacy questions. The American literature probably begins with The Naked Society (1964) by Vance Packard and The Privacy Invaders (1964) by Myron Brenton. And continually over the last thirty years publishers have been attracted by this more polemical genre. Not including scholarly contributions, a chronological, but incomplete, list of the more popular North American literature is as follows:

Edward Long, The Intruders: The Invasion of Privacy by Government and Industry (1967)
Jerry Rosenberg, The Death of Privacy (1969)
Arthur Miller, The Assault on Privacy (1971)
John Curtis Raines, Attack on Privacy (1974)
Arieh Neier. Dossier: The Secret Files They Keep on You (1975)
Alan Lemond and Ron Fry, No Place to Hide (1975)
Lester Sobel ed. War on Privacy (1976)
Robert Ellis Smith, Privacy: How to Protect What's Left of It (1979)
William C. Bier (ed), Privacy: A Vanishing Value (1980)
David Burnham, The Rise of the Computer State (1980)
Warren Freedman, The Right to Privacy in the Computer Age (1987)
David Linowes, Privacy in America: Is your Private Life in the Public Eye? (1989)
Jeff Rothfeder, Privacy for Sale (1992)
Erik Larson, The Naked Consumer (1992)
Steven Nock, The Costs of Privacy: Surveillance and Reputation in America (1993)
Deckle Maclean, Privacy and Its Invasion (1995)
Ann Cavoukian, Don Tapscott, Who Knows: Safeguarding Your Privacy in a Networked World (1996)
Beth Givens, The Privacy Rights Handbook: How to Take Control of Your Personal Information (1997)
Janna Malamud Smith and Elizabeth Maguire (eds), Private Matters: In Defense of the Personal Life (1997)
Ellen Alderman & Caroline Kennedy, The Right to Privacy (1997)
Chris Peterson, I Love the Internet, But I Want My Privacy Too! (1998)
Whitfield Diffie and Susan Landau, Privacy on the Line (1998)
Charles Sykes, The End of Privacy (1999)
Fred Cate, Privacy in the Information Age (1999)
Reg Whitaker, The End of Privacy (1999)
Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century (2000)
Jeffrey Rosen, The Unwanted Gaze: The Destruction of Privacy in America (2000)

I have grouped together here a literature that has been written from a diversity of perspectives, ranging from the journalism of David Burnham and Jeff Rothfeder to the civil libertarian approach of Arieh Neier, to the insights of David Linowes (the former chair of the US Privacy Protection Study Commission). The literature also encompasses a shifting concern about emerging technologies, from the concern for "snooping devices" in the 1960s, to the sophisticated trade in personal information revealed in Privacy for Sale to the contemporary concerns about the Internet in Privacy on the Line.

A parallel, though smaller, literature has also emerged in Britain with a similar tone and emphasis:

Donald Madgwick, Privacy under Attack (1968)
Malcolm Warner & Michael Stone, The Data Bank Society (1970)
Anthony A. Thompson, Big Brother in Britain Today (1970)
Donald Madgwick & Tony Smythe, The Invasion of Privacy (1974)
Paul Sieghart, Privacy and Computers (1976)
Patricia Hewitt, Privacy: The Information Gatherers (1977)

Ian Will, The Big Brother Society (1983)
Duncan Campbell & Steve Connor, On the Record: Surveillance, Computers and Privacy (1986)
Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order (1996b).
Stuart Goldsmith, Privacy: How to Live a private Life free from Big Brother's Interference (1997)

Perhaps the importance of this literature, however, lies in its cumulative impact and message. A steady flow of horror stories about the intrusive nature of modern technology, about the abuse and misuse of personal data, and about the size and interconnectedness of contemporary information systems has probably had a steady impact on public and political consciousness (Smith, 1993). Many of these stories are then picked up by the print and TV media. Big Brother imagery, together with accounts of how the powerless can be denied rights and services through the wrongful collection, use and disclosure of personal data certainly make good copy.

These images are also increasingly prevalent in popular culture. Gary Marx has written a perceptive analysis of the depiction of surveillance in art, songs, cartoons, advertisements, television, and films. He concludes that in an egalitarian, democratic society such as ours, we are ambivalent about the ramifications of surveillance. Omniscience, with its parallel to an all-seeing God, appeals to our sense of control, but we are fascinated and repelled by seemingly omnipotent power, particularly one that is mechanistic (Marx, 1996).

In general, the more journalistic literature tends to provide a quite crude picture of the overall nature and effects of surveillance. Its purpose is to draw attention to the complexity and scale of the problem, and to the weakness of existing safeguards. More empirical studies within individual sectors have more successfully exposed the operation and effects of surveillance practices.

Empirical Studies of Surveillance

In Privacy and Freedom, Alan Westin expressed concern that the development of powerful computers would lead organizations to engage in surveillance of individuals and groups on an unprecedented scale (Westin, 1967: 366). He cited historical examples of technologies developed for one use, often by the government, and then adopted by public and private interests for surveillance. Westin revised his analysis as result of studies conducted from 1970 to 1972. Westin oversaw a study for the National Academy of Sciences in which researchers conducted site visits and follow up contacts to 55 organizations, including government agencies engaged in law enforcement, as well as hospitals, the military, and private institutions such as businesses, schools, and religious bodies (Westin & Baker, 1972 :25). He and co-author Michael Baker concluded in Databanks in a Free Society (1972) that the use of computers had not, so far, led organizations to amass more individual personal information, and that organizations followed the same procedures in protecting, or not

protecting, individual privacy, as they had prior to the development of computers. Westin and Baker predicted that the limitations based on cost and complexity of third-generation computer systems would change in 1970's and 80's, and that new organizational rules and framework legislation would be needed at that point.

A contemporaneous study was James Rule's early comparative analysis of information systems in Britain and the United States (1974). Based on three British, and two American case studies of surveillance systems in both public and private sectors, Rule attempted to assess empirically the changes in surveillance capacity and the attendant implications for social control. In contrast to Westin and Baker, he concluded that the overall surveillance potential had grown with the advent of computerized record-keeping in both countries. On the other hand, surveillance systems at that time were limited in terms of the size of the files in the system, centralization, the speed of flow between points in the system, and the number of contact points between the system and the individual (1974: 37-40).

As technology has become smaller, less expensive, and more decentralized, analysts have reached rather different conclusions. Gary Marx's (1988) analysis of undercover police surveillance is a case in point. Marx demonstrates how incremental changes in technology, social values and the law have encouraged covert and deceptive police techniques with a variety of intended and unintended consequences. He demonstrates how all covert surveillance has the tendency to blur the distinction between law enforcement and the lawless activities it is supposed to curtail.

The range of new surveillance practices that Marx discusses allows him to suggest some more general characteristics of these new forms of social control: 1) The new surveillance transcends distance, darkness, and physical barriers; 2) It transcends time; its records can be stored, retrieved, combined, analyzed, and communicated; 3) It has low visibility, or is invisible; 4) It is often involuntary; 5) Prevention is a major concern; 6) It is capital rather than labor-intensive; 7) It involves decentralized self-policing; 8) It triggers a shift from targeting a specific suspect to categorical suspicion of everyone; 9) It is more intensive -- probing beneath surfaces, discovering previously inaccessible information; 10) It is more extensive -- covering not only deeper, but larger, areas. "The awesome power of the new surveillance," Marx summarizes, "lies partly in the paradoxical, never-before-possible combination of decentralized and centralized forms" (1988: 217-9). David Lyon (1992) later provided some perceptive reflections on the implications of Marx's analysis for the "maximum security society."

The decentralized, unplanned, incoherent nature of modern surveillance is echoed in other works written in the 1980s. Joseph Eaton's analysis of identity cards demonstrated how, on a de facto basis, Americans already have a national identification card system: "Some people think that the absence of a formal national identification (ID) system is one of the remaining bastions of our right to be let alone. But on a de facto basis, it has already been breached. Other than children, the mentally retarded, and the deceased, how many Americans are without either a social security card, a driver's license, a credit card, or all three of these documents?" (1986: 1-2). He goes on to argue that a truly comprehensive

national identity card would provide better protection against fraud, misuse and the invasion of privacy.

The analysis (though not the prescription) is echoed in a 1986 report from the US Office of Technology Assessment, Electronic Record Systems and Individual Privacy. It begins: "the widespread use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a de facto national database containing personal information on most Americans. And use of the social security number as a de facto electronic national identifier facilitates the development of this data base" (1986: 3). The point is effectively demonstrated through a careful analysis of the uses of new techniques for the analysis of personal data: computer matching, computer-assisted front-end verification, and computer profiling.

Roger Clarke found it necessary to coin a new word, dataveillance, to describe these new forms of surveillance that are facilitated, not by direct visual or audio monitoring, but by the manipulation of personal data. Roger Clarke, one of several Australian privacy analysts, has contended that the "Big Brother" scenario has not arrived because it is unnecessary: "ubiquitous two-way television a la 1984 has not arrived even though it is readily deliverable. It is unnecessary because dataveillance is technically and economically superior" (1989: 499).

There is a wide, and imperfectly understood, range of practices for the analysis of personal data currently used by modern governments. Dataveillance practices vary along five different dimensions: 1) whether personal or mass dataveillance is being conducted; the former involves the analysis of the records of individuals who have already attracted attention, the latter begins with no a priori knowledge of the subjects who may warrant attention; 2) whether the dataveillance is internal or external to the agency that initially collected the data; 3) whether the analysis is upfront or post-facto, that is whether the check is made before or after an individual receives a government benefit of service; 4) whether the analysis is conducted on a single variable, or a multiple number of variables (such as when profiling occurs); and 5) whether the practices have a negative or positive impact on individuals (Marx & Reichman, 1984; Clarke, 1989; Bennett, 1996a).

Another Australian writer, Simon Davies, the Director-General of Privacy International, has given some serious thought to the stages through which surveillance systems pass: "As a society becomes larger and more complex, as its links with other nations grow, and as its technological capacity increases, it is normal for it to creep up the surveillance scale" (Davies, 1992: 18). Restricted (Zone 1) Surveillance would only exist in the minimalist "nightwatchman" state. Conditional (Zone 2) Surveillance only exists after adequate debate and the introduction of appropriate safeguards. Routine (Zone 3) Surveillance exists in three principal areas, law enforcement, taxation and government benefits. Mass (Zone 4) Surveillance is a zone of "enforced, interactive and punitive surveillance" in which "most, if not all, aspects of people's movements, transactions, interactions and associations" are monitored. Total (Zone 5) Surveillance occurs when "people show an Orwellian willingness to support government control" (1992: 19-20). Davies argues that many developed countries, including Australia, have been rapidly

creeping up to the fourth level of surveillance. In a later article, Davies attempted to create a model that evaluates the collection, use, and disclosure of personal data as a means of measuring and comparing surveillance on a cross-national level (Davies, 1996a).

Surveillance and the Private Sector

The initial work on surveillance has largely focussed on the activities of the state. Hence, in the works of Rule, Marx, Clarke, Davies, and in the less scholarly work, there is at least an implicit assumption that the explanation for the rise in surveillance is chiefly located in the inherent (maybe pathological) tendencies of bureaucratic organizations to want to collect, organize, manipulate and control information. When focussed on the state, the roots of the problem tend to reside in the Weberian theory of rationalization, rather than in Marxist or Foucauldian perspectives.

Two more recent works, which have directed their attention as much to private sector practices, see rather different trends at work. Oscar Gandy's The Panoptic Sort (1993) draws upon a diversity of traditions to try to understand the implications for social control of new and sophisticated practices for the collection, classification, and manipulation of personal information by both public and private sectors. Marx, Ellul, Giddens, Weber, Foucault all contribute to an understanding of the system of disciplinary surveillance that continually seeks to identify, classify and evaluate individuals according to ever more refined and discriminating forms of personal data: "the panoptic sort is a difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technique that allocates options and opportunities on the basis of those measures and the administrative models that they inform" (1992: 15). His analysis leads him to the conclusion that real consumer choice can only be implemented through "Opt-In" rather than "Opt-Out" provisions. In later discussions he has written that attempts to control the use of technology through a regime of rights or a market will not work, because the choice is an illusion (Gandy, 1996).

David Lyon (1994) still employs more visual imagery to address much the same questions about surveillance in The Electronic Eye. He also contends that surveillance cannot be reduced to one social or political process, drawing inspiration from much the same literature, as does Gandy. Whereas Gandy relies on contemporary empirical analysis of the surveillance practices of modern corporate and bureaucratic organizations, Lyon adopts a more historical approach to link surveillance to theories of modernity, and to speculate on the possibilities and implications of a more communitarian post-modern condition, as a way to avoid the dystopic visions of both Orwell and Foucault. In this light, surveillance may have positive, as well as negative, ramifications. In a similar vein, Judith Perrolle looks at computer supported cooperative work systems, which create new opportunities for workplace surveillance through observation by *other employees*, and not the organization. She concludes that privacy in small groups is not merely the absence of surveillance, but a dynamic process, negotiated among the members of the group, and this must be born in mind in order to create an effective working environment (Perrolle, 1996).

Rohan Samarajiva, in analyzing the effect of new technology on business practices, has written that "Customized mass production makes customer relationships necessary, but it does not pre-determine whether they will be stable, productive relationships based on trust, privacy and consensual surveillance or pathological relationships based on coercive surveillance, mistrust, and anger" (Samarajiva, 1997: 300). New technologies can also cause us to redefine our notion of privacy, shrinking it in the face of perceived benefits to society, and expanding our understanding of the idea of the "public interest," beyond what could have been predicted (Davies, 1997). Diffie and Landau point out that that the dependence on modern telecommunications has made it easier to obtain others' secrets, at a time when people are more concerned about privacy. Paradoxically, even as Americans have accepted a right to privacy, the government and private businesses have greatly expanded the abilities and efforts to intrude on individual privacy (Diffie & Landau, 1998: 225-29).

The analysis of surveillance systems tries to locate the profound and macroscopic social trends from the temporal or idiosyncratic. But there are inherent dangers in drawing universal judgements from North American experience. The nature and extent of surveillance probably varies across nations, across economic sectors, across bureaucratic institutions. There is a valuable path of inquiry (at a more middle-range theoretical level) which attempts to locate and explain this observed variation. Political scientists have a potential contribution here.

For instance, the sharing of personal data between the agencies of the democratic state for whatever social or political purpose is hypothetically determined by the wider structural configuration of different states, even though the same technological, economic and bureaucratic forces may be at work. For example, it is no accident that computer matching (the comparison of personal data from different files to expose instances of waste, fraud and abuse) should have surfaced first in the United States. Here, public policy is administered through a loose collection of bureaus with very weak vertical lines of authority. This encourages horizontal linkages across government departments thus facilitating the sharing of data. In Britain, by contrast, where these practices are not so widely used, strong lines of hierarchical integration, bolstered by a departmental "esprit de corps" foster secrecy both vis-a-vis the general public, and in relation to other civil service departments. Strong institutional jealousies militate against the sharing of personal data for dataveillance purposes (Bennett, 1996a).

Thus the new surveillance may be determined by, and may impact, the internal structural organization of state institutions. It may also, of course, influence the relationship between public and private sector entities. It is becoming apparent that, for example, the files of credit reference agencies are sometimes used to check the eligibility for social services. Private financial institutions are increasingly being considered for the development of "smart cards" and for the dispensing of government benefits. Where do these forms of surveillance leave the distinction between the "public" and "private?"

These and other trends lead Philip Agre (1994) to the conclusion that a "capture" model is just as evocative as a "surveillance model" to represent the new commodification of personal information. This model is built upon linguistic rather than visual metaphors and has its roots in the disciplinary practices of applied computing rather than in the historical

experiences of the "surveillance state." "Information entrepeneurialism" is the term Kling and Allen use for the strategy businesses increasingly employ to gather data on customers, leading to new kind of surveillance, and social control, in a society of those with relatively few bonds (Kling & Allen, 1996).

In summary, the literature on surveillance leaves us with the overwhelming message that the quantity and quality of surveillance have changed. The volume of data collected and stored by both public and private organizations has facilitated a range of new practices that have developed incrementally and without much public attention or opposition. By the same token, the surveillance society is not one yet overseen by an omniscient "Big Brother." The formal or legal establishment of a comprehensive national identity system has nowhere been necessary. That system has developed through the uncontrolled decisions of thousands of decentralized public and private organizations, all making supposedly rational decisions that one more incremental invasion of privacy is a price worth paying for greater efficiency and/or profit.

Regardless of the roots and extent of modern surveillance practices, from a political standpoint, this increase in surveillance capacity can have a dysfunctional impact on the relationship between individuals and public and private institutions. Many new surveillance tools are predicated on an assumption that citizens cannot be trusted. Whether one is discussing video cameras in public places, e-mail monitoring in the workplace, computer matching to detect fraud, the consumer credit industry or any other contemporary practice, these systems can serve to increase the level of distrust between individuals and the public and private organizations with which they relate. There may be a circular process at work, whereby the increase in surveillance capacity reduces the level of societal trust and alienation, which in turn produces further deviant behavior, deemed worthy of further surveillance. As a political, rather than a psychological or sociological problem, the implications of excessive surveillance for the operation of the institutions of advanced democratic states requires further analysis from political scientists.

PRIVACY, DECISION-MAKING AND THE IMPACT OF NEW INFORMATION TECHNOLOGIES

The analysis of any attempt to promote more privacy in advanced industrial societies immediately raises profound issues about the deterministic or convergent impact of technology, and the relative autonomy of state policy-makers to control or regulate its more intrusive and dangerous effects. Political scientists have debated such questions at length in relation to the control of nuclear technologies, industrial pollution, television, and so on. Again, however, these questions have rarely been directly addressed with respect to privacy.

That is not to say that the commentary on the privacy implications of the new technology practices that have arisen since the 1960s has not been underpinned by some implicit assumptions about the relationship between technological forces, and organizational or individual choice. The analysis of technologies like computer matching, computer profiling, the development of smart cards, new telephone services (such as call-display),

integrated networks, electronic mail, genetic databanks, the "Clipper Chip" and so on, is frequently accompanied by reflections about the nature of the "technological imperative." In this context, the promotion of greater privacy is directly dependent on the ability of individual decision-makers to control these wider structural forces. The debate then raises the age-old conflict between voluntarism and determinism, and the issue of whether outcomes are shaped by structure or by human agency.

Technology and Political Theory

Theories about the relationship between technology and politics generally come in three broad categories. The first sees technology as an autonomous or deterministic force. Once technologies are set in motion, they tend to follow their own course independent of human direction. The theory in its purest form is normally associated with the writings of the French sociologist, Jacques Ellul (1964). But it has always been a powerful theme in political and social thought (Winner, 1977). At the other end of the spectrum we find a range of writings that believe that technology cannot be understood outside its social and political context, and therefore can never be regarded as an independent force. On the one hand, it may be shaped by the conscious and autonomous decisions of political agents. On the other, it may be shaped by existent organizational norms or standard operating procedures.

A third, more centrist body of literature, regards this as one big chicken-egg, or cart-before-the-horse debate. This middle position sees outcomes shaped by a complex dynamic interaction between new technologies and existing political and social practices. Here, the outcomes of information technology usage will reflect "the interactive relationship between technological developments, political decisions and existent organizational norms and practices. Technology sets boundaries to achievements, but within those limits, human choice and conflict have considerable latitude (Bennett, 1991: 64). Or as Ithiel de Sola Pool put it: "Technology shapes the structure of the battle but not every outcome" (Pool, 1983: 251). Westin (1980) uses a different analogy to make the same point, seeing technology as a kind of "projectile" propelled into organizations, and society, shaped by and shaping the existing "steel web" of rules and practices**.**

These theoretical positions rest heavily, of course, on prior conceptualization of the word "technology." It is now evident that information technology includes substantially more than the basic hardware and software that is commercially available. James Danziger and his colleagues, in their study of the use of computers in local government, talk of a "computer package" to denote an interdependence of people, equipment and machines (1982: 4-5). Thus the significant unit of analysis is the "technology practice," or the behaviors, rules, conditions etc. that surround the hardware and the software. The existence of a new technology can raise issues not previously foreseen.

Another argument that combines the determinist and bureaucratic control models is that of "function creep." A kind of organic growth is almost universally observed in the implementation of information technology in whatever field of operation. Social and political factors may determine the initial application of a technology. However, once a system is in place, it is rare for its continual growth ever to be reversed. The strategic

potential of the technology becomes more obvious to those who use it, but only after it has been implemented for some time. Winner stated the principle as follows: "once underway, the technological reconstruction of the world tends to continue" (1977: 208).

Those who would reject the determinist argument would probably view the privacy problem as stemming from the inherent pathologies of bureaucratic organization. Thus the problem is the acquisition and aggrandizement of power. These assumptions underpin, to some extent, talk about "surveillance states." Here is Michael Stone and Malcolm Warner, writing in 1969: "The computer has given bureaucracy the power of omniscience, if not omnipotence, by putting into its hands the power to know" (1969: 260). U.S. Senator Sam Ervin, the architect of the 1974 US Privacy Act, claimed that "officials at every level of our national life who make decisions about people for limited purposes seem possessed by a desire to know the "total man" by gathering every possible bit of information about him" (1971: 138). Robert J. Gallati, former Director of New York State's Identification and Intelligence System, was more direct: "If we wish to be scientific, it is obvious that we must have information -- lots and lots of data about oodles and oodles of persons and things" (Gallati, 1971: 42-3**).** Similarly, David Flaherty, quoting William Parent, writes: "One can today only acknowledge 'the continued and voracious expansion of the public and private sectors' appetite for more and more refined and integrated personal data at the expense of personal space and individual autonomy." (Flaherty, 1997: 187).

The perspective of those who root the essential privacy problem in the inherent corrupting influence of power is also more likely to be influenced by historical experiences. The technology is more likely to be regarded as a mere "tool" in states with more vivid memories of the abuse of political power. This is certainly a central motivation behind data protection law in continental Europe. A 1984 conference of data protection experts concluded that "one of the prime motives for the creation of data protection laws in continental Europe is the prevention of the recurrence of the experiences in the 1930s and 1940s with Nazi and fascist regimes" (Flaherty, 1984a: 5).

Those who have conducted any empirical research into the development and application of personal information systems tend, however, to adopt a more centrist position. Here is David Flaherty, writing in 1989: "Civil servants seek data on individuals to design and evaluate programs, to augment their prestige and power, and, as a product of a supposed technological imperative, to enable them to use the latest hardware and software" (1989: 13). Arthur Miller (1971: 21) articulates a "Parkinson's Law" of privacy invasion, similar to the notion of "function creep": "Technological improvements in information-handling capability have been followed by a tendency to engage in more extensive manipulation and analysis of recorded data."

The development and application of personal identification numbers can also be effectively understood as a process of "function creep." The pattern seems to be pretty consistent everywhere. Numbers such as the American Social Security Number, the Canadian Social Insurance Number (SIN), the Australian Tax File Number, and the British National Insurance Number, were originally introduced solely for the purpose of administering social benefits and unemployment insurance programs. Their utility as

identifiers for other purposes was then recognized by other public institutions. Gradually they have been used for a variety of unrelated purposes to the extent that they have been regarded as de facto universal identifiers.

In contemporary circumstances, the distinction between a technological decision, and a political decision is increasingly blurred. Computer code can have the equivalent controlling effect of legal code. Joel Reidenberg has spoken about a "lex informatica", and the consequent importance of politicizing and rendering transparent the political decisions that take place in the labs of Intel or Microsoft (Reidenberg, 1998, 2000).

Empirical Studies of Technology and Privacy

Empirical investigations into the development and effects of specific personal information systems also provide some insights into the processes of IT acquisition and development. One of the earliest, mentioned above, is Alan Westin and Michael Baker's project for the National Academy of Sciences, Databanks in a Free Society. Based on site visits to 55 government, commercial and non-profit organizations, the findings of this project indicated that the "content of computerized records about individuals has not been increased in scope compared to what was collected in their manual counterparts in the precomputer era" (1972: 244). They concluded that "pre-computer rules have not been altered in computerizing organizations; rather, customary practices have been reproduced with almost mirrorlike fidelity" (1972: 253). Westin and Baker forecast in 1972 that the cost of computing and data storage would be dramatically reduced, and that interfacing would be easier (Westin and Baker, 1972: 317-31). They therefore called for the creation of new privacy laws and other standards at that time, rather than waiting for more studies or for policies on data and privacy to develop (Westin and Baker, 1972: 339-403). This study was initially cited as evidence that the computer was not the villain, and that attention to the privacy issue had been exaggerated. But the Westin and Baker findings were based on 1970-72 data, when the cost of computerization was far greater, and file integration more difficult, than it is today (Regan, 1981: 78-9).

The later analysis of criminal justice information systems conducted by Ken Laudon for the Office of Technology Assessment (US, OTA, 1982), revealed that some of Westin and Baker's warnings had not been heeded. This study found that the use of criminal history records for purposes other than those for which they were collected was extensive and growing. It was found that criminal record checks were conducted for employment and licensing purposes, especially for applicants to positions entrusted with the care of persons who are likely to be vulnerable (especially children, the elderly, the mentally handicapped). The incremental use of a technology in place for seemingly legitimate social purposes, by the early 1980s, had amounted to a surveillance system over which there were few controls and about which there was much concern (Laudon, 1986).

Donald Marchand's The Politics of Privacy, Computers and Criminal Justice Records (1980) also found that the use of criminal justice records outside the traditional confines of

the criminal justice system was enormous and increasing. Privacy was viewed as one largely symbolic way that the political system may exercise some control over the "technology reception" process: "The recognition of this right, in view of increased organizational record-keeping and computerization and the adverse effects of these activities on individuals, has meant that privacy is not only a concrete right to be reconciled with competing social goals and rights, but, stated abstractly, also is a political resource" (Marchand, 1980: 88). A careful empirical analysis of the case of criminal justice records in the United States allows Marchand to examine the role that privacy plays within the wider interaction between technological development, organizational norms, and political choice.

Evidence from public opinion polls also suggests a strong, if poorly understood, fear of computer technology. Distrust of technology appears to be closely tied to distrust of institutions (Harris-Westin, 1990: XXII). Around two-thirds of the American public agreed in the 1991 update survey that "if privacy is to be preserved, the use of computers must be sharply restricted in the future" (Harris-Westin, 1992a: 20). By 1999, 94% of Americans polled said that they were concerned about "possible misuse" of their personal information, and 80% agreed with the statement that "consumers have lost control over how personal information is collected and used by companies" (IBM-Harris: 70-71, 165, 249; Westin, 2000). Evidence also suggests, however, that those who know how to use computers are less afraid of the "1984" scenario that those who do not (Dutton & Meadow, 1985). But users of the Internet report higher incidences of invasion of privacy, and are more likely to refuse to give out information, or decide not purchase a good, because of concerns about privacy (IBM-Harris: 16-19, 69-72, 164-65, 248-49; Westin, 2000). Business elites are also far less likely to regard computers as a threat to privacy than are the general public (Harris-Westin, 1990: 83).

It is, however, a mistake to believe that information technology is necessarily antithetical to privacy interests. Recent advances in the field of public-key encryption have demonstrated that some technologies can also be privacy friendly (Katz, 1987: 84; Chaum, 1985; 1992; Cavoukian, 1999). David Chaum's basic point is that common identifiers such as social security numbers inevitably involve a trade-off between security and individual liberties. But advances in microelectronics, and in the development of secure "digital signatures" allow people to adopt a different (but verifiable) identifier to every organization they do business with. Theoretically, this would make "dossiers" impossible and unnecessary. Organizations would also benefit from increased security and lower record-keeping costs.

Herbert Burkert sees four different types of privacy-enhancing technology concepts: subject-oriented, object-oriented, action-oriented, and system-oriented. Subject-oriented concepts are those that attempt to reduce the ability to personally identify the subject. Object-oriented concepts are those seek to create the electronic equivalent of cash so that the object of the transaction is not identifiable. Transaction-oriented concepts address the secrecy of records of the transaction, and system-oriented concepts attempt to integrate the other elements, coming as close to anonymity as possible. Burkert acknowledges that such concepts are contingent on a particular understanding of "privacy," while a more political definition would require designers to provide for social interaction and "electronic

democracy." The very existence of such technologies, he concludes, should lead all social scientists, regulators and privacy practitioners to think more about the need for social innovation (Burkert, 1997).

The obstacles to the application of encryption technology are probably political, economic and psychological rather than technical. However, encryption can be a two-edged sword. The US Government's decision in the early 1990s to pursue the "Clipper Chip" as a national standard for encryption has been severely criticized by privacy experts for its ability to enhance the government's capabilities for electronic surveillance. It has also met with stiff opposition from the private sector which sees it as discouraging the development and export of new cryptographic technology (Barlow, 1994). Diffie and Landau provide a more recent description of the debate over the Clipper Chip, (Diffie & Landau, 1998: 205-25) as do David J. Phillips (Phillips, 1997), and Lance J. Hoffman (1990).

Thus encryption technology is also susceptible to the process of "function creep." The bureaucratic imperative to make the most efficient use of public resources (including personal information) has been overwhelming within recent conditions of high deficits, increased levels of criminality and neo-conservative economics. Thus, if a technology is available, the likelihood is that it will be used for one of these wider social and governmental purposes. That, I would argue, is the history of computer matching, of the development of identification numbers, and of the application of new telecommunications services. The same trend is being witnessed, on a larger and more ubiquitous, canvas with the development of personal data gathering techniques on the Internet.

PRIVACY AND PUBLIC POLICY

Political scientists may also see privacy protection as a regulatory policy, the development of which may tell us something interesting about how different states manage technological change. In this light, the issue raises a set of fairly traditional questions for the policy analyst: How did privacy reach the political agendas of different states? How did interest groups and policy communities articulate the issue? How was it pursued through the legislative process of different countries? How were policy instruments chosen for its enforcement and implementation? How has privacy (data protection) policy been implemented? How has its success been evaluated?

Privacy and Policy Development in Comparative Politics

The analysis of privacy as a political issue can yield some fascinating insights into the capacities of different countries with different institutional arrangements and policy legacies to define recognize and respond to, a common problem. It is, therefore, ideally suited to the approaches and techniques of the comparativist. It permits a nice distinction between the "persistent, generic, and transnational from the conditional, particular, and country-specific" (Bennett, 1992: x). It also allows a combination of the analytical approaches of international relations with those of the comparativist.

The number of works that have analyzed the development of privacy policy within an explicitly comparative framework is, however, very limited. The earliest was Priscilla Regan's (1981) Ph.D. dissertation on approaches to privacy protection in Britain and the United States, and related articles (1984, 1990). David Flaherty's (1979, 1989) comparisons of the implementation of data protection law in the United States, Canada, Sweden, West Germany and France also includes brief sections on policy development in these five countries.

This gap in the literature offered me the opportunity to conduct a thorough analysis of policy development in my 1986 Ph.d dissertation, which was later published as Regulating Privacy. Here, the formation of data protection policy in the United States, Britain, Sweden and West Germany, was studied in terms of an analytical framework of convergence and divergence. In the 1970s and 1980s, the international pressures for convergence were slowly overwhelming distinctive national policy differences. The major divergences related to the different policy instruments through which the information privacy principles were enforced and implemented. I extended this analysis in "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?," (Bennett, 1997). Although Regulating Privacy was written before regulatory responses to the Internet, the development of a global information infrastructure simply reinforced the internationalization of the threat to personal privacy. Moreover, the EU Data Protection Directive, passed in 1995, is binding on member states and encourages convergence not just in the area of policy but in the implementation of those policies. In addition, because it bans data transfers to other countries unless those countries have "adequate" levels of protection, it has been a force promoting the consideration of similar laws in countries such as Canada, New Zealand, Australia and Japan and in the promotion of further self-regulation in the United States (Bennett, 1997).

Viktor Mayer-Shonberger extends this analysis to argue that European data protection laws have gone through several distinct stages. The European Data Protection Directive has motivated the development of the fourth generation of data protection statutes. Along the way, however, the meaning of data protection and the content of law have shifted to address different technological changes and challenges and to encompass shifting philosophical meanings. More recent approaches have moved “away from simplistic versions of informational privacy as a negative liberty and toward broad participatory rights of informational self-determination, supported and enhanced by a renaissance of direct regulatory involvement” (Mayer-Schonberger, 1997: 235). Beyond this, a special issue of *the International Review of Administrative Law and Sciences* on data protection I guest edited with Charles Raab and Wim B.H.J. van de Donk contains a number of insightful articles on privacy regimes the U.S., Britain, Canada, the Netherlands, and the EU.

Most of the comparative literature, however, is within the field of comparative law, is more descriptive and normally makes little attempt to understand the law within the broader social, cultural or political contexts of different countries (e.g. Hondius, 1975; Bing, 1978; Schwartz, 1989). Nevertheless, the privacy literature can be used to draw some wider conclusions about privacy as a regulatory policy and how it has been treated in different advanced industrial states.

Privacy and the Political Agenda

The analysis of how issues hit agendas, how they become "issues whose time has become" (Kingdon, 1984) has attracted the attention of many political scientists. There are some common patterns. In all countries, to some extent, plans for the computerization of government information systems and for the extension of universal identification numbers caused the most notable concern. Another common variable is the role of expertise; in most countries, it seems, one or two key figures gained a reputation for being the experts on privacy and data protection. A body of knowledge circulated amongst this elite, and was readily available to any governmental decision-making body.

But there are also some interesting variations. In some countries, the issue emerged steadily and quietly as an elite of experts gradually and skillfully articulated the problem and convinced key policy-makers that legislation was necessary; this was largely the pattern in Sweden, for instance. In others, a "triggering mechanism" was necessary, such as the Watergate scandal in the United States, or the uproar over the "Safari" personal information system in France (Flaherty, 1989: 166). In the countries that have legislated in the 1980s and 1990s (for example Britain, the Netherlands, Canada), it is probable that economic considerations, relating to the trade implications of transborder data flows, were key motivations.

In the United States, Priscilla Regan studied three areas: information privacy, communications privacy, and psychological privacy. She found that in each case, a technological development such as wiretapping, the invention of the polygraph, or computerization of records was the key event in getting an issue on the public agenda. Groups would enter the policy arena for the first time, generally not out of a concern for privacy, and interact with other interested parties. Issues around which the media can tell "interesting stories," become prominent, and the issue itself becomes distorted by media focus. Finally, for an idea to be acted upon politically, there should be at least a latent public interest in it (Regan, 1995: 174-81).

The role of interest groups should be further analyzed. In all states, civil liberties and consumer associations played some part in articulating the concerns. More interesting work could focus on the role of professional associations (such as those in the medical, legal and financial fields), and on the different coalitions that it was necessary to build in order to inject data protection policy into different sectors. In this regard, there has been a little analysis of the role that industry played in lobbying for the British Data Protection Act of 1984 (Bennett, 1992: 91). Regan's (1993) case study of the passage of the *Electronic Communications Privacy Act* in the United States is also evidence of the importance of the building of coalitions of interest groups (in this instance between key industry associations and the civil liberties lobby) for the passage of privacy legislation.

In her 1995 study, Regan found that the role of interests dominated policy formulation and adoption, to the exclusion of the ideas regarding privacy that originally drove the debate. As new technology raised privacy concerns, and therefore possible legislation, interested parties were able to redefine the issue from one of "privacy" to one that answered their concerns. These interests were not just private interests but even federal agencies, which, for example, desired to maintain control over their own information

systems, or avoid legislative restrictions on their use of technology. Interested groups, particularly private ones, used popular public ideas, such as government efficiency, or adequate law enforcement, to hide the true reasons for their positions. Regan concludes that the creation of a policy community formed to mobilize support for privacy was critical for the passage of legislation. These scholars, lawyers, journalists, elected officials, staff members and other advocates gave testimony, held conferences, formed committees and associations, raising awareness of privacy problems in the United States, and reacting to changes in technology. The existence of this community was particularly important because no other groups, even those with an interest, such as Common Cause or labor unions, were able to take the lead on the issue (Regan, 1995: 173-211).

As attempts to strengthen privacy law in the private sector gain momentum at the international level (through such instruments as the EU Directive on Data Protection) and within North America, important opportunities will arise for the analysis of the political influence of the "data-intensive" industries. These include sectors such as credit reference, insurance, banking and particularly direct marketing. There is compelling evidence that the latter has been especially active in lobbying against the "informed consent" provisions within the EU Directive (Raab & Bennett, 1994; Regan, 1999). American businesses and politicians anxious to continue to do business in Europe and keep the computing and communications industry growing have recently negotiated some "Safe Harbor" rules to allow uninterrupted flows of personal data from Europe to the US to those companies that self-certify to a number of privacy principles. The politics of this issue obviously take on a very different character when the resource to be regulated (personal data) is one upon which many organizations rely for their very existence.

Privacy and Policy Adoption

By far the most attention in the privacy literature has been paid to the next "stage" in the policy-making process, namely the formal legislative history. Several books and articles give brief accounts of how the privacy or data protection bill became a privacy or data protection law. One especially interesting story was how the U.S. Privacy Act of 1974 came to be passed without a provision for a Privacy Commission (see Flaherty, 1984b; Regan, 1984; Linowes & Bennett, 1986). The story reflects a typical American process of bargaining and logrolling. Differences in the Senate and House versions of the Privacy Act required last-minute compromise. The Privacy Commission, originally proposed by Senator Ervin, was ultimately removed in favour of an analytical body, the Privacy Protection Study Commission, and oversight by the Office of Management and Budget and by Congress. Regan has also examined the process leading to the passage of the Computer Matching and Privacy Protection Act of 1988, the Electronic Communications Privacy Act of 1986, and the Employee Polygraph Protection Act of 1988. She discusses in detail the stages leading to passage of legislation, including rising public concern, Congressional committee hearings, lobbying by interested groups, and compromise between houses of Congress and the President (Regan, 1995).

David O'Brien (1979) adds an interesting chapter on "Personal Privacy as an Issue of Public Policy" to his otherwise fairly traditional public law analysis of the subject. He

attempts to place American federal privacy policy within a framework for understanding the informational flows that are demanded by all information policy (including the Freedom of Information Act) (O'Brien, 1979: 221). Privacy, for O'Brien, is as much a political ideal as a legal right or an existential condition.

Comparative legislative histories are also briefly traced for the countries that Flaherty (1989) studies. Other short accounts appear in several other works on Britain (Campbell & Connor, 1986), on West Germany (Simitis et al., 1981; Bull, 1984), on Australia (Davies, 1992), several states in Europe and Quebec (Le Bris & Knoppers, 1997) and so on. The juxtaposition of these stories, I have argued, allows the political scientist to say something more generally about styles of public policy-making (1992: 229-38). In some states, the politics were largely consensual (e.g. in Sweden); in others major battles were fought (such as in Australia and West Germany). In some, the process was short (such as in France); in others it was drawn-out (e.g. in Britain and the Netherlands). The process by which Canada has more recently moved toward data-protection legislation has revealed fascinating features of a national policy-making process that is characterized by ambiguity and incrementalism (Bennett, 1996b.)

The chief battles in most countries were fought not over the principles of fair information practice, but over the methods and structures through which they would be enforced. A cross-national convergence around these principles can be contrasted with a divergence over the "policy instruments" that different states chose. This allows the political scientist to examine a central hypothesis of the comparative public policy literature, which suggests that states have a basic repertoire of "tools" that they apply in any problem-solving situation (Hood, 1986). I found that there was some support for this hypothesis in the data protection case (Bennett, 1992: 195-200); some states do have some fixed notions about which policy instruments "fit" into the wider institutional setting. On the other hand, the specific powers granted to some data protection agencies were also influenced by political bargaining between elected and unelected officials (Bennett, 1988b). The later development of data protection policy in Canada also reflects this same pattern, a consensus on international privacy principles, but a choice of policy instrument that is deeply embedded in Canada's administrative and political culture (Bennett, 1996b).

Implementation of Privacy Law

The experience of the implementation of privacy and data protection law also permits an interesting interrogation of theories and hypotheses drawn from wider political science literature. Regan's (1984: 19) statement about the dilemma of implementation certainly provides a very realistic picture of the difficulties facing policy-makers in this area. With reference to the United States and Britain, she demonstrates how, "when implementation questions are left unresolved in policy design, bureaucratic concerns dominate the implementation stage; yet, when implementation questions are resolved in policy design, bureaucratic concerns dominate the formulation stage." This dilemma arises in this peculiar area of regulatory policy, in which the regulated (i.e. bureaucratic agencies) are also the

regulators. I explored these dilemmas further in an analysis of the implementation of the Canadian Privacy Act (Bennett, 1999).

The continuing battles over the development of new personal information systems between bureaucracy and data protection agencies are traced in detail in Flaherty's (1989) volume. The conditions for successful implementation are inductively drawn out at the end of the study. These can be summarized in the following way: 1) a constant review and adaptation of the statutory framework; 2) an expertise in the capabilities of new technology; 3) a separate policy instrument with a permanent, relatively small, dedicated, administratively expert staff whose responsibilities for onerous licensing and registration tasks are minimized; 4) a single privacy advocate at the head of the agency who knows exactly when to use the carrot and when the stick; and 5) a supportive public, media and legislative opinion. Flaherty does not like part time commissioners, or collective committees (such as the Commission Nationale de L'Informatique et Libertes in France). In summary, he concludes that data protection agencies should not be a kind of "miniparliament that seeks to settle the appropriate balance internally ... Emphasis should be on the antisurveillance side of the balance, since the forces allied against privacy, or at least in favor of effective surveillance, are generally so powerful" (1989: 391). Spiros Simitis, the prominent Data Protection Commissioner from the state of Hessen, drew some similar conclusions about the necessary elements of any regulatory system in an influential 1987 article. Schwartz (1992), too, uses knowledge of the German data protection regime to critique the incoherent American response to the problem.

Flaherty has had experience in the implementation of privacy protection law, as Information and Privacy Commissioner for the Province of British Columbia. Flaherty has reported less resistance from the bureaucracy than he predicted in 1989, though conceding that he was still in his "honeymoon" phase and that budget cutbacks could affect his ability to function. He still considers data protection commissioners "alarm systems" for privacy, and has adopted a functional and empirical approach to the job rather than a formalistic one. He agrees with Simitis in avoiding public or private confrontation, and searching for consensus. He writes that the area where his views have changed the most since 1989 is in the need for regulatory, and not simply advisory, powers, for his office (Flaherty, 1997: 167-91). Flaherty has more recently concluded that as the World Wide Web, e-commerce and other technologies have grown, concerns over data protection increase, as the need for the state to intervene on behalf of citizens rises. However, he writes: "I am not a fan of solely bureaucratic and statutory solutions. . . . Individuals will have to fend for themselves wherever it is possible to do so" (Flaherty, 1999: 19-38, 31).

It would be very profitable, however, if someone could apply some of the political science literature on implementation to privacy and data protection law. Flaherty does cite Daniel Mazmanian and Paul Sabatier's (1983) framework for effective policy implementation. Other more contemporary works may yield more rewarding hypotheses. Charles Raab (1993), for example, has contended that some models for implementation analysis rely too much on a top-down approach, in which variables are deductively analyzed as a kind of checklist. This model may not be suitable for the analysis of data protection. Rather, more dynamic approaches would be more sensitive to the process of mutual learning

which is, of course, indispensable to any data protection agency and especially to those that have to rely on advisory rather than regulatory strategies. Raab has looked further at the problems of implementing data-protection laws in Britain, an approach which helps us focus on enforcement organizations such as the British Registrar, and not simply on the concepts and ideals behind privacy laws. He finds the record of success decidedly mixed, but concludes that "privacy is a fragile plant," and that Britain's conflict-resolving style "could be injured by the competing imperatives which it purports to hold together. . . ." (Raab, 1996: 509).

The final set of questions for the policy analyst have to do with evaluation. Do privacy or data protection laws achieve their stated goals? There has been some attempt by data protection agencies to think about possible performance measures to justify their resources. Policy evaluation techniques have been developed and applied in many other areas of regulatory policy, many of which are admittedly more amenable to more quantitative or objective assessment methods. Nevertheless, political scientists have given careful thought to performance measures, and similar analysis can probably be applied to privacy and data protection too. The initial why, what, how and who questions that any policy evaluation would need to address have been outlined in a recent article (Raab & Bennett, 1996).

One of the most systematic surveys of adherence to data protection law in the Netherlands found high levels of non-compliance. Further, the authors found that factors accounting for high levels of data protection were non-statutory - such as self-interest, professional culture, attitudes of management, and technology. They report that enforcement was weak and that the law was out of touch with reality at the shop-floor level, and conclude that general regimes are not as useful as legislation or instruments specifically targeted in particular areas (van de Donk & van Duivenboden, 1996: 513-534).

Herbert Burkert has also written about the success of data protection in the public, as opposed to private sectors. He hypothesizes that such laws contribute to the modernization of public administration agencies, by facilitating the quality and legitimacy of the move to computerized handling of records (Burkert, 1997: 557-568). And Robert Gellman has evaluated U.S. privacy law. While recognizing the difficulty in measuring the success of such laws, he concludes that the failures he did perceive were the result of a lack of interest, incentive and enforcement (Gellman, 1997: 215). The evaluation of success is also closely related to issues of distribution: who gets how much privacy (or conversely surveillance) in advanced industrial states is also a controversial question (Bennett & Raab, 1997).

The task is a complex one. But it is important to begin to grapple with the essential issue of what constitutes "policy success" in this area, and who should evaluate that success and how. This depends on how we observe, and maybe measure, protection. Among other things, we need to question the assumptions behind instruments like the EU Directive that countries can be ranged on a clear scale, with those with "high" levels of protection at the top, those with "adequate" protection in the middle, and those with "inadequate" protection at the bottom.

PRIVACY, CAPITALISM AND THE INFORMATION MARKET

The assumption behind most of the literature cited above is that, however framed, privacy is an important democratic right that the state has some obligation to protect through regulatory policy. In the United States, with some exception, that obligation generally extends only so far as the personal information held by federal and state governments. In others, the policy problem is seen as the same wherever large quantities of personal data are stored -- in both public and private sectors. But in virtually every advanced industrial country, a privacy (or personal data protection) policy has been fashioned. Privacy is now almost universally seen as a political problem.

Some authors, however, arguing from economics or public choice assumptions contend that, as privacy is an inherently private good, it can be better protected through individual responses and market-based mechanisms. Those who have argued this case and challenged the conventional wisdom have been lone voices. However, as the scale and complexity of the information economy increases, so more privacy analysts have been looking to market-based mechanisms in the belief that the "information superhighway" of the future will likely be impossible to oversee and regulate.

One key assumption behind this position is that privacy is not a final good, but an intermediate or instrumental value: "Under this approach, people are assumed not to desire or value privacy or prying in themselves but to use these goods as inputs into the production or income of some other broad measure of utility or welfare" (Posner, 1978a, p. 19). Flowing from this distinction between ends and means, Posner contends that "with regard to ends there is a prima facie case for assigning the property right in a secret that is a byproduct of a socially productive activity to the individual if its compelled disclosure would impair the incentives to engage in that activity; but there is a prima facie case for assigning the property right away from the individual where secrecy would reduce the social product by misleading the people with whom he deals" (1978b: 403).

The economics of personal information are controversial. Richard Posner's initial (1978a, 1978b) exposition of the theory drew much criticism (e.g. Bloustein, 1978). The policy implications of this analysis lead to common law solutions, in which there has never been recognized a right for individuals to conceal discrediting information about themselves. Posner's analysis does, of course, rely on a clear and objective distinction between true and false, or harmful and harmless, information. Others have shown that the nature of the information is not the crucial element, but rather the context in which it is stored. My name and address in the telephone directory is normally harmless; that same information on a list of bad credit risks is capable of doing me considerable harm.

These, and other, critiques (e.g. Stigler, 1980; Gould, 1980) of the theory of information privacy, and the "fair information practice" doctrine that underpins the statutory approach has, however, led to a more recent search for marketplace solutions to the privacy problem. These explorations take a variety of forms, and do not necessarily follow the logic

presented by Posner. Nevertheless, the space for debate about alternative approaches has opened up, especially given recent trends in marketing.

The Personal Information Market

Changes in the fundamental nature of marketing are responsible for shifting concerns about personal privacy (Culnan, 1993). Many have noted the trend away from mass-based advertising toward more targeted, direct marketing strategies. Sophisticated "psychographic" techniques, which allow a refined analysis and profiling of consumer attitudes and lifestyles have directed the search for more and more precise information about individual preferences and behaviours (Smith, 1994: 76-7). Direct marketers argue that they can only reduce the nuisance value of "junk-mail" by collecting and sorting more precise and accurate data about individual consumers. Nevertheless, companies in these "information-intensive" sectors are well aware that consumer privacy concerns can disrupt their businesses. Consumers are not, therefore, powerless, although the depth and scope of potential consumer pressure for privacy has yet to be clearly understood.

Simpson Garfinkel points out that marketers and consumers *both* wish to cut down on junk mail and unwanted phone calls to consumers, common forms of mass marketing which consumers find annoying and which does not often yield results (Garfinkel, 2000: 155). In addressing this problem, consumers are trying to restrict marketing practices, while marketers are building more refined lists in an effort to better target consumers. Marketers purchase lists of names and addresses from organizations they think may include people interested in their product, and also use official "change of address" forms, supermarket discount card lists, product registration lists, and even hospital records to assemble their target lists. Oscar Gandy gives the name "Panoptic sort" to the technology that collects, processes and shares information about individuals and uses it to control their knowledge of and access to goods and services (Gandy, 1993: 15). And Reg Whitaker calls the constant profiling of individuals by commercial interests "the decentered, consensual Panopticon" (Whitaker, 1999: 139).

Seth Godin, of Yahoo, is highly critical of the “interruption marketing” that is reflected in billboards, radio and TV ads, and which rarely reaches interested parties. Personalized marketing, using refined lists, direct mail, phone solicitations and Internet banner ads may be more efficient, less intrusive, and more likely to offer a product the consumer is interested in. In a throwback to an earlier age, marketers hope to use a technique called "permission marketing," whereby sellers market only to those buyers who have expressed an interest in hearing from them. Godin writes that those engaged in "interruption marketing," are trapped in a Catch-22. They must spend more and more to get the attention of the consumer, yet they only increase clutter of ads which the consumer is likely to ignore (Godin, 1999: 37-38). Godin sees permission marketing as advantageous for both parties, as consumers do not like to be interrupted and marketers need the attention of consumers who are actually interested in their product and urges marketers to build on their relationships with customers, to eventually create loyalty, so their customers become their "friends."

A recent survey showed that 60% of American respondents thought that personalized marketing was a “good thing” (IBM-Harris Survey; *Privacy and American Business*, 2000). On the other hand, 94% of respondents said they were concerned about

"possible misuse" of their personal information, and nearly 30% said they had been the victims of a violation of their privacy as a consumer. Consumers had confidence in banks and healthcare industries, but very little in Internet sales companies, when it came to protecting their privacy. A majority had taken steps to protect their privacy, by for example, refusing to give out information (78%) or asking to have their name removed from a list (58%). Those using the Internet were even more privacy assertive (IBM-Harris Survey; *Privacy and American Business,* 2000).

Simpson Garfinkel also sees intensive personalized marketing as dangerous, resulting in ever more junk mail (including for the deceased) and fraught with the potential for abuse. He cites one case where a supermarket threatened to use a customer's buying habits against him in a lawsuit, and the sale of health or shopping records could be used in denying insurance. He writes: "Runaway marketing has become a nonstop campaign of corporate sponsored harassment. This campaign will eventually be extended to every man, woman, and child on this planet. It must be stopped." (Garfinkel, 2000: 156). The problem takes on a new dimension when the philosophy of personalized marketing is combined with the interactivity of the Internet, and the enhanced capability to track consumers preferences and choices through the analysis of "clickstream data." Recent stories about Doubleclick, an online advertising service, and America Online possibly using information they have about amassed about web surfers for marketing purposes are probably precursors of the conflicts to come (Fraase, 1999: 147).

Jim Taylor and Watts Wacker argue that we are at a watershed moment in history, where humanity will make a leap forward and all assumptions regarding society and economics will be cast aside (Taylor & Wacker, 1997: 7) They urge companies to extol the benefits of "membership", and deliver something for the exclusivity of their own valued customers. They predict that privacy management will be a growth industry, both for information given out and taken in, as "there will be no greater status tool than having someone manage your privacy for you, . . . no greater proof of your worth than that the flood of connectivity directed toward you is beyond your capacity to control yourself" (Taylor & Wacker: 225-26).

Privacy Solutions within the Personal Information Market

The recognition of the increased value of personal information in the marketplace has led to a number of policy approaches each designed to promote enhanced levels of privacy, by recognizing and promoting the inherent incentives for businesses to gain and maintain the trust of its customers (Culnan, 1999).

We see, firstly, a burgeoning debate (especially in North America) about the incentives that business might have to promote "privacy friendly" practices. There is plenty of evidence that industries within the credit, financial, direct-marketing and telecommunications sectors, for instance, have recognized the economic importance of promoting an image of being responsible users of personal information through the implementation of voluntary codes of practice (Bennett, 1995). The development of mail and telephone preference services which allow consumers to "opt-out" of direct marketing lists can also be explained by similar motives. Although, as Jeff Smith demonstrates in his

recent empirical analysis of the personal data practices of American business, the extent and nature of that recognition is variable. The process by which businesses develop policies to control their personal data holdings is generally a "wandering and reactive one" (1994, p. 55).

If there is a business incentive to promote privacy-friendly practices then common codes of conduct might potentially spread throughout the economy in the same way that product and performance standards have been applied in other areas. Hypothetically, certification and registration processes can be administered through accredited standards-setting bodies. Privacy would then spread as market pressures, consumer demands, government procurement policies, international forces and so on, would force business to adopt the privacy code and verify to an independent auditor that it does what it says it does (Bennett, 1995). There is evidence that this is happening, as online certification processes have been developed through organizations such as TRUSTe and Better Business Bureau online. But the progress of self-regulation is distinctly uneven, and the development of privacy commitments, privacy codes, privacy standards and privacy seals not necessarily cumulative. Privacy is only in interests of business under certain conditions. And as Lawrence Lessig points out: "Norms can be effective regulators. But a necessary condition of their success is that the community of norm enforcers include those who bear the cost of the behavior being regulated" (Lessig, 1999: 159). One can question whether this indeed happens with respect to privacy.

A second approach is to establish (in law) personal information as a form of property, of which there is a number of proposals. Ken Laudon believes that the conceptual foundations of the fair information principles doctrine are outdated due to changes in the nature of the marketing economy, facilitated by changes in the capacity and speed of modern computer and communications technologies. The fair information practices regime was developed to deal with the privacy problems inherent in a relatively small number of large-scale mainframe databanks, rather than a fluid, decentralized and networked computing environment. Where one personal information system begins, and another ends is becoming impossible to define. He therefore believes that personal information should be regarded as a form of property, in which the individual has not only a "mere juridical or administrative interest" but a stronger property interest (Laudon, 1996: 92). He contends that "to ensure the protection of privacy beyond 2000, we should consider market-based mechanisms based upon individual ownership of personal information and National Information Markets (NIM) where individuals can receive fair compensation for information about themselves" (1996: 92).

James Rule and Lawrence Hunter come from a sociology background to argue the benefits of a somewhat different market-based solution to the sale and trading of personal data (Rule & Hunter, 1999). They advocate legislation that would create a property right over commercial exploitation of personal information by which "no information could legally be sold or traded from any personal data file, for any commercial purpose, without express permission from the person concerned (1999: 170). They would also be guaranteed the option to insist on royalties in exchange for the commercial release of personal data. This would arguably generate a new kind of business -- information brokers who would represent individuals' interests in the treatment of their personal information. Thomas Peters also

argues that the best way to protect information in the future will be to promote a market in which consumers own their information and receive fair compensation for its use (Peters, 1999: 118).

A third and related approach is to implement a property rights regime through the technology of cyberspace. Lessig has been the most recent advocate of such an approach, arguing for a "machine-to-machine protocol for negotiating privacy protections" (1999: 160). A property regime, he argues, is very different from a liability regime, because a "property regime requires negotiation before taking; a liability regime allows a taking, and payment later…..Property protects choice; liability protects transfer." Technologies (such as the P3P project from the World Wide Web Consortium) are perhaps able to create an architecture, not possible in the past, that will allow individuals to negotiate the circumstances under which their personal information may be collected and used. The role of the law is to establish that such a negotiation must occur.

Other scholars have explored the way that cyberspace facilitates the view of consumers that their personal information is a commodity. John Hagel and Marc Singer, two executives with McKinsey & Company, argue that there is a coming privacy backlash, which is not simply about intrusion but also due to a sense that people should be paid for the use of their information (Hagel & Singer, 1999). They write that new technologies will allow consumers to take control of their information, and that "infomediaries" will act as agents in protecting privacy while marketing personal information (Hagel & Singer: 18-20).

A final approach is based on the assumption that personal information has variable "value" depending on the type of institution that collects it. In this vein, Eli Noam has proposed a multi-tiered approach to privacy protection, in which certain levels of privacy not developed through legislation or constitutional interpretation would be "left to the market to allocate" (Noam, 1994: 35). These conclusions stem from Noam's own work on New York telecommunications privacy.

Each of these authors starts from different ideological and methodological assumptions to perceive a different crisis to come to these very different forms of market solutions. Laudon perceives an inherent weakness in FIPS doctrine; Noam emphasizes a rapidly changing technological environment within communications; Rule and Hunter see a crisis for consumer choice and empowerment. Lessig is informed by the power of computer code to enable consumer choice. Hagel and Singer are inspired by the potential of the Internet and the growth in electronic commerce. Each also have studied different institutions and technologies, in which the record-keeping relationships pose subtly different privacy problems, requiring different solutions (see also Bibas, 1994).

Moreover, each also proceeds from the observation that information surrendered in the course of applying for a government service, purchasing goods, using computer or communications technology and so on may be appropriated by third parties who normally have not engaged in any direct transaction with the data subject. Third parties (such as list-brokers and their telemarketing clients) are thus classic "free-riders" in the economy. There is a misallocation of the costs and benefits, because these third-parties consume a common property without covering the externalities related to its extraction and use (Lawson, 1995).

Posner and others of the Chicago school would contend that as privacy is only an intermediate good, there are no costs incurred when a third-party appropriates that personal information, unless privacy is necessary to prevent some final harm. Thus the imbalance in the allocation of costs and benefits in the information marketplace is an illusion, because the loss of privacy is not a basic "cost" if individuals have "nothing to hide." This critique would explain why it is a sociologist like Rule, believing that privacy is a fundamental right (a "final good" in economics terms), who has proposed a property-based solution to the exploitation of personal information in the information marketplace.

From a civil libertarian stance, the debate about market forces is incidental to the central issue that privacy should be a "public good." Consumers may have some bargaining power with a direct marketing firm that wants to trade lists; citizens, however, have no bargaining power when faced with a warrant or any other potentially privacy-invasive technique backed up by the sanctions of the state (Rotenberg, 1994). Simon Davies has an uncompromisingly negative view of an information market. He writes that "the process of commodification is inimical to privacy," because every measure of privacy protection is interpreted as a cost to the consumer: "Placing privacy in the free market environment along with such choices as color, durability and size creates an environment in which privacy becomes a costly "add-on" (Davies, 1997: 160).

CONCLUSION: POLITICAL ECONOMY AND THE PRIVACY DEBATE

There is a large literature about privacy, a good deal of which tackles questions of central importance to the disciplines of political science and economics. However, the number of academic political scientists or economists who have been cited in this chapter has been few. There are a number of reasons for this. First, political science, and especially American political science, tends to gravitate towards institutions, that is agencies with rules, personnel and budgets that can be empirically observed. Given the absence of a privacy or data protection commission in the United States, the issue has floated around a vast and diverse collection of congressional committees and executive agencies, all of which have other and generally more significant responsibilities. The second reason is that privacy tends to span the traditional subfields within political science. It is an issue of political theory, of public policy-making, of political behavior, of public administration, of comparative politics, and of international relations. To study the "politics" of privacy, as I have discovered, requires a certain, though inevitably superficial, familiarity with the conversations at these "separate tables." Finally, the paucity of academic economists cited can probably be explained by the strong disciplinary tendencies towards sophisticated quantitative methods. In this vein, there is a large literature on the economics of information. That analysis has, however, been conducted on a higher theoretical and methodological plane and has rarely, if ever, influenced the debate about privacy.

The dominant task of the privacy community has always been to analyze emerging technologies and organizational practices, analyze their impact on privacy and then to

fashion the appropriate regulatory response. These debates have generally been reactive rather than anticipatory. Understandably, they have been focussed on the pressing practicalities of the moment. This is perhaps more true today than in the 1960s. The cumbersome mainframes of thirty years ago were discrete and uncomplicated compared with the perplexing variety of new technologies that contemporary privacy analysts have to get their minds around.

The annual reports of the world's privacy commissioners, as well as their annual conferences, offer a glimpse of the shifting and expanding privacy agenda. They now discuss an increasing range of different technologies, most of which were never anticipated by national data protection laws nor contemplated as a responsibility for the data protection authority. At the September, 1999 Conference, Privacy Commissioners discussed the rapid developments in the growth of the Internet and genetics, among others (21st International Conference, 1999: 1-10.). New areas of concern also include biometric identification, web sites which surreptitiously collect information, encryption, video-surveillance, personal tracking devices, the needs and new abilities of law enforcement agencies, the abuses of privacy by the news media, and e-commerce and the unregulated international world of cyberspace (International Conference, 1999). By and large, neither our data protection authorities nor the relatively small (but growing) group of international privacy advocates have the resources to anticipate technological developments and research their various impacts. (For a list of recent Data Protection Agencies' and Privacy Commissioners' Annual Reports available in English, see Appendix).

As a result of this rapidly shifting landscape, the discourse about the politics of privacy tends to be overly reactive and descriptive. The privacy community understandably spends a lot of time and effort describing for each other the nature of the respective privacy laws, their scope and coverage, their treatment of tricky definitional problems, the powers they grant to the commissioners and so on. Comparative legalistic analysis has reached the point where journals such as Privacy Laws and Business can publish regular and very useful league tables on the worldwide state of data protection law. This approach reflects the predominance of legal scholarship, in which questions are confined to reviewing the state of the law in different countries and pointing out inconsistencies or inadequacies as new technologies enter society and challenge existing regulations. In the 1990s, non-legal solutions, such as self-regulatory instruments and privacy enhancing-technologies, have entered the debate. The privacy community is now fond of referring to a mosaic of different policy instruments that all need to be applied in privacy is to be effectively implemented (Bennett & Grant, 1999: 7).

Potential Contributions from Political Science

How then can political scientists and economists contribute to the debate about how best to protect the privacy of individuals in the 21st century? I would identify four key areas worthy of further research and analysis.

A first set of questions relates to policy development. As a consequence of the reactive nature of the current discourse, the analysis of privacy and public policy has been largely ahistorical. That is not to say that the value of privacy has not been analyzed using

historical methods. The most thorough example is Westin's dissertation of 1965, discussed in detail above (see "Historical and Cultural Traditions," supra). Westin analyzed privacy in five different eras: Periclean Athens, Rome in the second century, Europe in the 13th century, England from 1603-1650, and the early years of the United States. David Flaherty wrote a thorough study in 1972 titled Privacy in Colonial New England (Flaherty, 1972) in which he observed that the Puritans supported privacy in religious devotion and in the courtroom (Flaherty, 1972: 14-15). But, he noted, Puritans also suppressed privacy in favor of communal goals and adherence to a strict code of behavior. As the Puritan movement waned, one result was a greater acceptance of the demand for more personal privacy (Flaherty, 1972: 17).

Two other examples are David Seipp's The Right to Privacy in American History (1978), and Robert Ellis Smith's Ben Franklin's Web Site, a historical study of privacy in America from the earliest Colonial times through the present day (Smith, 2000). Smith notes the lack of privacy in Colonial New England observed by David Flaherty (Flaherty, 1972) and the earnestness of government record keeping even then. Of course, given the relatively small population, it was also easier to find privacy at that time, and citizens let authorities know when they had gone too far (Smith, 2000: 15-18). Concluding with an examination of the Internet, Smith writes "[M]uch of the strength of the Internet from 1990 to 1994 was its lack of inhibitions and regulations. It truly was an electronic frontier, more like a Western cowboy town than the electronic strip mall it became after 1994" (Smith, 2000: 351).

Through the analysis of privacy, historical methods have certainly been able to illuminate the social conditions of our ancestors, and demonstrate that privacy is a deep-seated and intrinsic human concern. However, in our focus on the latest technology, the latest law, the latest international agreement and so on, we tend not to see the policy issues in historical perspective. If we reflect on these historical developments, we may conclude that, even though there are still enormous weaknesses in some of the laws, the issue has come a long way in a relatively short period. A historical perspective can also help us understand the origins of current proposals. The European Data Protection Directive, for example, is the culmination of a set of processes that were originally set in motion in the early 1970s. It is the latest instrument of policy convergence, and builds upon previous international agreements that harmonized law on the level of some very general principles. The EU Directive directs a magnifying glass on a variety of more specific divergences in European data protection. This Directive would not have been possible without earlier harmonization efforts and the structures and processes that were set in place in the 1970s (Bennett, 1997).

A second contribution lies in comparative studies. I mean this in two different senses. On the one hand, there has been very little systematic comparison of how different states with different cultures and institutions have responded to these same technological challenges. We should continually reflect on how the same problems are resolved in different countries, and moreover what this then says about their approach to privacy protection, their institutional capacities to manage technological change, and their national cultures. Data protection is a marvelous issue for these kinds of comparative studies. A recent comparative study of workplace privacy in Canada, the United States, France and the UK draws some very interesting comparative conclusions about larger patterns of employee-labour relations in these four countries (Craig, 1999). There is enormous scope for analysts to take a technology that has diffused around the advanced industrial world and to investigate

and attempt to explain similarities and difference in national responses.

Systematic comparison can also shed light onto important cultural differences. In particular, when we focus too much on the state of the law, we may ignore the fact that the statutory or legal context is just one factor that influences the behavior of those in public and private organizations that process personal data. There are other more elusive, but sometimes more important, cultural and institutional factors that are seldom recognized. There are, for example, different administrative cultures in Western societies. Some of these, like those of Germany, are traditionally deferential to rules and administrative norms. I would argue, as does Flaherty, that this administrative culture makes the task of the data protector somewhat easier. In countries such as the United States, on the other hand, there is less of a centralized civil service mentality. Administration is more open to outside interests and personnel. Data protection policy has to be implemented within a more fragmented, less hierarchical, administrative system (Gellman, 1993).

Another aspect of a nation's culture can have an important impact on privacy protection. Political scientists have long tried to classify cultures according to whether they are deferential to authority, or more prone to participation, complaint, protest and so on. It is at least hypothetically true that countries whose citizens are less deferential to authority are going to be less trusting of agencies to handle personal information with care and propriety, and more prone to complain to relevant authorities. The cultural context within which data protection law needs to be implemented can, nevertheless, be lost when we focus too narrowly on the wording of law.

Another significant factor overshadowed by the legalistic emphasis of our conversations is the overall structural or institutional arrangements of government. This affects the position of data protection on the political and administrative agenda in a variety of ways. For instance, the relations between political and administrative agencies create distinctive styles of governance. The more consensual and accommodating styles of countries like Sweden are more conducive to anticipating developments and providing appropriate responses, than the more conflictual, fragmented and unpredictable style of a place like the United States. These and other institutional and cultural factors have profound comparative influences on the development and implementation of privacy and data protection policy. Sometimes they tend to be forgotten in the discussions over the most appropriate legal and regulatory responses to the latest technological intrusion.

Comparative political science can also contribute in one other sense. Our discourse is non-comparative in that it tends to be discussed as a discrete, compartmentalized issue. It has become what policy analysts call a distinct policy sector characterized by: a separate set of statutory instruments; regulatory bodies established to implement these laws; a circle of legal experts; a small group of journalists ready to publicize information abuses; a growing academic community with expertise in data protection and privacy; and a range of international arenas in which the policy community can exchange ideas and collaborate. The result of this "sectorisation" of the policy is that very little comparison is made with other related fields, such as consumer protection, environmental protection and so on. We often lose sight of the fact that much can be learnt about the implementation of privacy

regulations from the analysis of other regulatory fields that have less obvious connections.

So further comparative studies are necessary. These could be cross-national, in which the capacities of different states to manage the same technological challenge are compared and evaluated. They could be cross-technology, in which the responses of one state to different privacy invasive practices are compared (see, Regan, 1995.) They could also be cross-sectoral, in which the responses of different economic interests are compared (Bennett, 1995; Schwarz & Reidenberg, 1996). Comparative analysis is necessary both to escape American ethnocentrism, and to provide insights into larger theoretical questions about the capacity of democratic states to manage technological change.

A third set of questions relate to the choice and evaluation of different policy instruments. In the 1970s and 1980s these questions were predominantly legal ones. Today, however, a variety of different approaches are available: privacy-enhancing technologies to permit secure and anonymous personal data transactions, market approaches to encourage self-regulation, international conventions and agreements, as well as a greater role for social movements and privacy advocacy (Bennett & Grant, 1999: 7). With a "mosaic of potential solutions" (Cavoukian and Tapscott, 1995: 180), further questions are raised about how these different choices relate one to another. The tradition of studying "policy instruments"˜ or the "tools of government" (Hood, 1986) in political science may assist in determining how these different approaches might attain the various policy goals related to privacy protection.

With regard to self-regulatory instruments, for example, political science and indeed economics can contribute to our understanding of the circumstances under which business might adopt privacy policies in a voluntary manner. A number of hypothetical variables might influence corporate decision-making here: the threat of regulation, the level of publicity about the company's practices, the need to trade (and therefore communicate personal data) over international borders, and the market structure within that particular industry.

Moreover, how do we know whether public policies on privacy are "working"? What measures of policy success can be empirically determined and presented? What do these measures "measure"? Lessons can be drawn from related regulatory fields to provide insights into these questions.

Political science has long been divided over the differences between normative and empirical methods. The former concentrates on what ought to be; the latter on what is. In other terms, a distinction is drawn between theory and practice, often with the implication that theoretical debate and analysis is overly abstract and of no practical importance in the "real world" of business or government. However, these are false dichotomies. Good social science research employs theory to examine and draw conclusions about social events and phenomena. Observation should be informed by theory, and should inform theory. While a large and diverse range of literature has been incorporated into this review, very few works have seriously tried to advance our understanding through the empirical examination of hypotheses informed by wider theoretical propositions about the relationship between the

state, the market and the individual. At the heart of the privacy problem lies the question of power. It is, therefore, an inherently and inescapably political problem.

THE LITERATURE SEARCH

The literature cited in this survey has been compiled from a variety of different sources. A large portion (especially that on data protection) has been cited in previously published works (especially, Bennett, 1992). This has been supplemented by an extensive search for relevant works gleaned through the bibliographic search conducted for the Human Genome Project by scholars at the Center for Social and Legal Research, and by suggestions from scholars associated with this project.

A more systematic, though far less useful, search was conducted within the more general political science literature. In particular, the reference publication ABC Pol. Sci., which contains hundreds of journals and 150,000 articles in the area of political science was consulted for the last fifteen years and relevant articles noted. Also searched were PAIS, a database of social science journals, and JSTOR, a database containing the text of ten political science journals, thirteen economics journals, and nineteen others. Very little, however, was found when the following standard political science journals were searched: The American Political Science Review, the Journal of Politics, the American Journal of Political Science, Comparative Politics, Comparative Political Studies, British Journal of Political Science, Political Science Quarterly, European Journal of Political Research, Canadian Journal of Political Science. A browsing through the indexes of a collection of contemporary introductory textbooks on American politics also revealed a paucity of references to privacy.

APPENDIX

Recent Data Protection Agencies and Authorities Annual Reports in English:

Commission d'accès à l'information du Québec. Annual Report 1998 – 1999. An Abridged Report. Quebéc: CAI, June 1999. www.cai.gouv.qc.ca/angl2.htm

Data Protection Registrar of Switzerland (Eidgenössiger Datenschutzbeauftragter). 5th Annual Report of the Data Protection Registrar. Berne: PFPD, 1998.

Data Protection Registrar of the United Kingdom. 1999 – The Fifteenth Annual Report of the Data Protection Registrar. Wimslow: DPR, February 2000. Wood.ccta.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def30802566360045bf4d/

Information and Privacy Commissioner of British Columbia. 1998 – 1999 Annual Report. Victoria: IPC, July 1999. www.oipcbc.org/publications/annual/oipcbc_annual_report98-99.pdf

Information and Privacy Commissioner of Ontario. 1998 Annual Report. Toronto: IPC, 1999. www.ipc.on.ca/web_site.eng/our_role/ann_reps/ar-98/ar-98e.htm

Office of the Privacy Commissioner of Australia. Eleventh Annual Report on the Operation of the Privacy Act. Sydney: PC, October 1999. www.privacy.gov.au/publications/index.html

Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary. 1998 Annual Report. Budapest: OBH, 1998. www.obh.hu/adatved/idexek/1998/TARTALOM.htm#c

Privacy Commissioner of Canada. Annual Report 1998–99. Ottawa: PC of Canada, July 1999. www.privcom.gc.ca/english/02_04_07_e.htm

Privacy Commissioner of New Zealand. 1997 Annual Report. Wellington: PC, 1998. www.privacy.org.nz/recept/ar1997_1.html

Registratiekamer. Annual Report 1998 (English Summary). The Hague: Registratiekamer, June 1998.

State of Hawaii, Department of the Attorney General, Office of Information Practices. Annual Report 1999. Honolulu: OIP, 1999.

REFERENCES

ABC Pol Sci: A Bibliography of Contents: Political Science and Government. Santa Barbara, Ca: ABC-CLIO.

Agre, Philip E. 1994. "Surveillance and Capture: Two Models of Privacy," The Information Society 10: 101-127.

Agre, Philip E. & Rotenberg, Marc A., eds. 1997. Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Aldrich, Robert. 1982. Privacy Protection Law in the United States. Washington D.C.: U.S. Department of Commerce, National Telecommunications and Information Administration.

Alderman, Ellen and Caroline Kennedy. 1997. Ther Right to Privacy. New York: Vintage Books.

Allen, Anita L. 1985. Uneasy Access: Privacy for Women in a Free Society. Totawa, NJ: Rowman and Littlefield.

Allen, Anita L. 1997. "Genetic Privacy" in Rothstein, Mark A., ed., Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. New Haven: Yale University Press.

Allen, Anita L. & Erin Mack. 1990. "How Privacy Got its Gender," Northern Illinois University Law Review 10: 441-78.

Almond, Gabriel A. 1988. "Separate Tables: Schools and Sects in Political Science," PS: Political Science and Politics 21: 828-42.

Almond, Gabriel A. & Sidney Verba. 1965. The Civic Culture. Boston: Little Brown.

_____. 1980. The Civic Culture Revisited. Boston: Little Brown.

Arndt, H.W. 1949. "The Cult of Privacy," Australian Quarterly XXI: 69-71.

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

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

Benn, Stanley I. & Gerald F. Gaus, eds. 1983. Public and Private in Social Life. New York: St. Martin's Press.

Bennett, Colin. J. 1988a. "Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States," Governance 1: 415-41.

_____. 1988b. "Regulating the Computer: Comparing Policy Instruments in Europe and the United States," European Journal of Political Research 16: 437-66.

_____. 1991. "Computers, Personal Data and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s," Science, Technology and Human Values 16: 51-69.

_____. 1992. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca: Cornell University Press.

_____. 1995. Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association. Rexdale, Ont.: Canadian Standards Association.

_____. 1996a. "The Public Surveillance of Personal Data," in David Lyon and Elia Zureik, eds., Computer, Surveillance, & Privacy. Minneapolis: University of Minnesota Press.

_____. 1996b. "Rules of Road and Level Playing Fields: the Politics of Data Protection in Canada's Private Sector," International Review of Administrative Sciences 62: 479-92.

_____. 1997. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?," in Agre, Philip & Rotenberg, Marc A., eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

_____. 1999. "Where the Regulated are the Regulators: Privacy Protection within the Contemporary Canadian State" in Bruce G. Doern, Margaret M. Hill. Michael J. Prince and Richard J. Schultz (eds), Changing the Rules: Canadian Regulatory Regimes and Institutions (Toronto: University of Toronto Press, 1999).

_____, Wim B.H.J. van de Donk, and Charles Raab. 1996. "The Politics, and Policy of Data Protection: Experiences, Lessons, Reflections and Perspectives," International Review of Administrative Sciences 62: 459-464.

_____ and Raab, Charles. 1997. "The Distribution of Privacy Risks: Who Needs Protection?," The Information Society , 14: 263-74.

_____ and Grant, Rebecca, eds. 1999. Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press.

Bensman, Joseph & Robert Lilienfeld. 1979. Between Public and Private: The Lost Boundaries of the Self. New York: Free Press.

Bibas, Steven A. 1994. "A Contractual Approach to Data Privacy," Harvard Journal of Law and Public Policy 17: 591.

Bier, William C. (ed). 1980. Privacy: A Vanishing Value? New York: Fordham University

Press.

Bing, Jon. 1978. "A Comparative Outline of Privacy Legislation," Comparative Law Yearbook 2: 149-81.

Bloustein, Edward J. 1978. "Privacy is Dear at any Price: A Response to Professor Posner's Economic Theory?," Georgia Law Review 12: 429.

Boling, Patricia. 1994. "Privacy as Autonomy vs. Privacy as Familial Attachment: A Conceptual Approach to Right to Privacy Cases," Policy Studies Review 13: 91

Boling, Patricia. 1996. Privacy and the Politics of Intimate Life. Ithaca: Cornell University Press.

Brenton, Myron. 1964. The Privacy Invaders. New York: Coward-McCann.

Brin, David. 1998. The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? Reading, MA: Addison-Wesley.

Bull, Hans Peter. 1984. Datenschutz oder die Angst vor Dem Computer. Munchen: Piper.

Burkert, Herbert. 1982. "Institutions of Data Protection: An Attempt at a Functional Explanation of European National Data Protection Laws," Computer Law Journal 3: 167-88.

Burkert, Herbert. 1997. "Privacy-Enhancing Technologies: Typology, Critique, Vision," in Agre, Philip E. & Rotenberg, Marc A., eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

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

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

Cate, Fred. 1997. Privacy in the Information Age. Washington, D.C.: The Brookings Press.

Cavoukian, Ann and Don Tapscott. 1996. Who Knows? Safeguarding your Privacy in a Networked World. New York: McGraw-Hill.

Cavoukian, Ann. 1999. "The Promise of Privacy-Enhancing Technologies: Applications in Health Application Networks," in Bennett, Colin J. & Grant, Rebecca, eds. Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press.

Chaum, David. 1985. "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM 28: 1030-44.

_____. 1992. "Achieving Electronic Privacy," Scientific American August 1992: 96-101.

Clarke, Roger A. 1989. "Information Technology and Dataveillance," Communications of the ACM 31: 498-512.

Council of the European Union (EU). 1995. Common Position on the Protection of Individuals in Relation to the Processing of Personal Data and the Free Movement of Such Data. Brussels: European Union.

Council of Europe (CoE). 1981. Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe.

Craig, John D.R. 1999. Privacy and Employment Law. Oxford: Oxford University Press.

Crick, Bernard. 1964. In Defence of Politics. London: Penguin Books.

Culnan, Mary J. "How Did They Get My Name? An Exploratory Study of Consumer Attitudes Toward Secondary Information Use," MIS Quarterly 17: 341-63.

_____. and Don Bies. 1999. "Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the 21st Century," in Colin Bennett and Rebecca Grant (eds), Visions of Privacy: Policy Choices for the Digital Age Toronto: University of Toronto Press.

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

Danziger, James N., William H. Dutton, Rob Kling, and Kenneth L. Kraemer. 1982. Computers and Politics: High Technology in American Local Governments. New York: Columbia University Press.

Davies, Simon. 1992. Big Brother: Australia's Growing Web of Surveillance. Sydney: Simon & Schuster.

Davies, Simon. 1996a. "Surveying Surveillance: An Approach to Measuring the Extent of Surveillance," in Lyon, David & Zureik, Elia eds., Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

_____. 1996b. Big Brother: Britain's Web of Surveillance and the New Technological Order. London: Pan

_____. 1997. "Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in Agre, Philip E. & Rotenberg, Marc. Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Diffie, Whitfield, & Landau, Susan. 1998. Privacy on the Line The Politics of Wiretapping

and Encryption. Cambridge: The MIT Press.

Dutton, William & Robert Meadow. 1985. "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties and the Democratic Process." Report prepared for the US Congress Office of Technology Assessment (OTA). Washington DC: OTA.

Easton, David. 1965. A Framework for Political Analysis. Englewood Cliffs: Prentice-Hall.

Eaton, Joseph W. 1986. Card-Carrying Americans: Privacy, Security and the National ID Card Debate. Totowa, NJ: Rowman & Littlefield.

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

Ervin, Senator Samuel J. Jr. 1971. "Privacy and Government Investigations," University of Illinois Law Forum: 138-150.

Etzioni, Amatai. 1994. Spirit of Community: Rights, Responsibilities and the Communitarian Agenda. New York: Simon and Schuster.

Etzioni, Amitai. 1999. The Limits of Privacy. New York: Basic Books.

Flaherty, David H. 1972. Privacy in Colonial New England. Charlottesville: University Press of Virginia.

_____. 1979. Privacy and Government Data Banks: An International Perspective. London: Mansell.

_____. 1984a. Nineteen Eighty-Four and After. Final Report of the Bellagio Conference on Current and Future Problems of Data Protection. London: University of Western Ontario Privacy Project.

_____. 1984b. "The Need for an American Privacy Protection Commission," Government Information Quarterly 1: 235-58.

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

_____. 1997. "Controlling Surveillance: Can Protection be Made Effective?," in Agre, Philip E. & Rotenberg, Marc eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

_____. 1999. "Past, Present and Future," in Bennett, Colin J. & Grant, Rebecca, eds., Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto

Press.

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

Fraase, Michael. 1999. Information Eclipse: Privacy and Access in America, St. Paul, MN: Arts & Farces.

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

Fried, Charles. 1968. "Privacy," Yale Law Journal 77: 475-93.

Gallati, Robert R.J. 1971. "The New York State Identification and Intelligence System," in Alan F. Westin, Information Technology in a Democracy. Cambridge: Harvard University Press.

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

_____. 1996. "Coming to Terms with the Panoptic Sort," in Lyon, David & Zureik, Elia eds., Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Garfinkel, Simpson. 2000. Database Nation: The Death of Privacy in the 21st Century, Sebastopol, CA: O'Reilly Press.

Gavison, Ruth. 1980. "Privacy and the Limits of the Law." Yale Law Journal 89: 421-71.

Gellman, Robert M. 1993. "Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," Software Law Journal VI: 199-238.

_____. 1997. "Does Privacy Law Work?" in Agre, Philip E. & Rotenberg, Marc A., eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Giddens, Anthony. 1985. The Nation State and Violence. Berkeley: University of California Press.

Givens, Beth. 1997. The Privacy Rights Handbook: How to Take Control of your Personal Information. Avon Books.

Godin, Seth. 1999. Permission Marketing: Turning Strangers into Friends, and Friends into Customers, New York: Simon & Schuster

Goldsmith, Stuart. 1997. Privacy: How to Live a private Life free from Big Brother's Interference. London: Medina;

Gotlieb, Calvin C. 1996. "Privacy: A Concept Whose Time has Come and Gone," in Lyon,

David & Zureik, Elia, eds., Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Gould, J.P. 1980. "Privacy and the Economics of Information," Journal of Legal Studies, 9: 827

Hagel, John III; Singer, Marc. 1999. Net Worth: Shaping Markets When Customers Make the Rules. Boston: Harvard Business School Press

Harris, Louis, & Alan F. Westin. 1979. The Dimensions of Privacy: A National Opinion Research Survey of Attitudes toward Privacy. Stevens Point, Wisc: Sentry Insurance.

_____. 1990. The Equifax Report on Consumers in the Information Age. Atlanta: Equifax Inc.

_____. 1992a. Harris-Equifax Consumer Privacy Survey. Atlanta: Equifax Inc.

_____. 1992b. The Equifax Canada Report on Consumers and Privacy in the Information Age. Montreal: Equifax Canada Inc.

_____. 1994. The Equifax Canada Report on Consumers and Privacy in the Information Age. Montreal: Equifax Canada Inc.

_____. 1998. Privacy Concerns and Consumer Choice: A P&AB Survey. New York: Louis Harris & Associates.

Hewitt, Patricia. 1977. Privacy: The Information Gatherers. London: National Council for Civil Liberties.

Hixson, Richard F. 1987. Privacy in a Public Society: Human Rights in Conflict. New York: Oxford University Press.

Hoffman, Lance J., ed. 1990. Rogue Programs: Viruses, Worms, and Trojan Horses. New York: Van Nostrand Reinhold.

Hondius, Frits W. 1975. Emerging Data Protection in Europe. Amsterdam: North Holland.

Hood, Christopher C. 1986. The Tools of Government. Chatham, N.J.: Chatham House.

IBM-Harris Multi-National Consumer Privacy Survey. 1999. New York: Harris Interactive. *See also* http://www.ibm.com/services/e-business/priwkshop.html

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

International Conference on Privacy and Personal Data Protection, 21st Annual, in Conjunction with the International Data Protection Commissioners' Meeting. 1999. "Privacy of Personal Data, Information Technology & Global Business in the Next Millennium:

Conference Proceedings," Office of the Privacy Commissioner for Personal Data, Hong Kong SAR, China.

Katz, James E. 1987. "Telecommunications and Computers: Whither Privacy Policy?" Society 25: 81-6.

Kingdon, John W. 1984. Agendas, Alternatives, and Public Policies. Boston: Little Brown.

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

Larson, Erik. 1992. The Naked Consumer. New York: Holt.

Lasswell, Harold. 1950. Politics: Who Gets What, When, How. New Haven: Yale University Press.

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

_____. 1996. "Markets and Privacy." Communications of the ACM Vol. 39, No. 9: 92-104.

Lawson, Ian. 1995. Privacy and the Information Highway: Regulatory Options for Canada. Ottawa: Industry Canada.

Le Bris, Sonia & Knoppers, Bartha Maria. 1997. "International and Comparative Concepts of Privacy," in Rothstein, Mark A., ed., Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. New Haven: Yale University Press.

Lemond, Alan and Ron Fry. 1975. No Place to Hide: A Guide to Bugs, Wiretaps, Surveillance, and other Privacy Invasions. New York: St. Martin's.

Lessig, Lawrence. 1999. Code and Other Laws of Cyberspace. New York: Basic Books.

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

Linowes, David F., and Colin J. Bennett. 1986. "Privacy: Its Role in Federal Government Information Policy," Library Trends 31: 19-42.

Lipset, Seymour Martin. 1990. Continental Divide: The Values and Institutions of the United States and Canada. New York: Routledge.

Long, Edward V. 1967. The Intruders: The Invasion of Privacy by Government and Industry. New York: Praeger.

Lyon, David. 1992. "The New Surveillance: Electronic Technologies and the Maximum Security Society," Crime, Law and Social Change 18: 159-172.

_____. 1994. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press.

Lyon, David & Zureik, Elia, eds. 1996. Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Maclean, Deckle. 1995. Privacy and Its Invasion. Westport, CT: Praeger.

Madgwick, Donald. 1968. Privacy Under Attack. London: National Council for Civil Liberties.

Madgwick, Donald & Tony Smythe. 1974. The Invasion of Privacy. London: Pitman.

Marchand, Donald A. 1980. The Politics of Privacy, Computers and Criminal Justice Records: Controlling the Social Costs of Technological Change. Arlington, Va: Information Resources Press.

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

_____. 1996. "Electric Eye in the Sky: Some Reflections on Surveillance and Popular Culture," in Lyon, David & Zureik, Elia, eds., Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Marx, Gary & Nancy Reichman. 1984. "Routinizing the Discovery of Secrets: Computers as Informants," American Behavioral Scientist 27: 423-452.

Mayer-Schonberger, Viktor. 1997. "Generational Developments of European Data Protection Norms," in P. Agre and M. Rotenberg, Technology and Privacy: The New Landscape Cambridge: MIT Press.

Mazmanian, Daniel A. & Paul A. Sabatier. 1983. Implementation and Public Policy. Glenview, Ill: Scott, Foresman.

McClosky, Herbert J. 1980. "Privacy and the Right to Privacy," Philosophy 55: 17-38.

McClosky, Herbert J and Alida Brill. 1983. Dimensions of Tolerance: What Americans Believe about Civil Liberties New York: Russell Sage Foundation.

Mill, John Stuart. 1859 (1991). On Liberty and Other Essays John Gray ed. Oxford: Oxford University Press.

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

Moore, Barrington Jr. 1984. Privacy: Studies in Social and Cultural History. Armonk, NY: M.E. Sharpe.

Moore, Barrington Jr. 1998. "Privacy," Society 35: 287.

Neier, Aryeh. 1975. Dossier: The Secret Files They Keep on You. New York: Stein and Day.

Noam Eli M. 1994. Privacy in Telecommunications: Markets, Rights and Regulations. Monograph in "Ethics in Telecommunication" Series. Cleveland: Office of Communication, United Church of Christ.

Nock, Steven. 1993. The Costs of Privacy: Surveillance and Reputation in America. New York: De Gruyter.

O'Brien, David M. 1979. Privacy, Law, and Public Policy. New York: Praeger.

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

Packard, Vance. 1964. The Naked Society. New York: David McKay.

Parent, William A. 1983. "Privacy, Morality and the Law," Philosophy and Public Affairs 12: 269-88.

Parker, Richard. 1974. "A Definition of Privacy," Rutgers Law Review 27: 275-96.

Pateman, Carole. 1970. Participation and Democratic Theory. Cambridge: Cambridge University Press.

_____. 1983. "Feminist Critiques of the Public/Private Dichotomy," in S. I. Benn & G.F. Gaus eds. Public and Private in Social Life. New York: St. Martin's Press.

Pennock, J. Roland & John W. Chapman. 1971. Privacy. Nomos XIII. New York: Atherton Press.

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

Peters, Thomas A. 1999. Computerized Monitoring and Online Privacy. Jefferson, NC: McFarland & Co.

Peterson, Chris. 1998. I Love the Internet, but I want my Privacy too. Prima Publishing.

Phillips, David J. 1997. "Cryptography, Secrets, and the Structuring of Trust," in Agre, Philip E. & Rotenberg, Marc A., eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Plesser, Ronald L. 1991. Privacy Protection in the United States. Washington D.C.: Piper & Marbury.

Pool, Ithiel de Sola. 1983. Technologies of Freedom: On Free Speech in the Electronic Age. Cambridge: Harvard University Press.

Posner, Richard A. 1978a. "An Economic Theory of Privacy," Regulation May-June 1978: 19-26.

_____. 1978b. "The Right to Privacy," Georgia Law Review 12: 393-422.

_____. 1993. "Blackmail, Privacy & Freedom of Contract," University of Pennsylvania Law Review. 141, No. 5 : 1817

Poster, Mark. 1990. The Mode of Information. New York: Polity Press.

Powers, Madison. 1994. "Privacy and the Control of Genetic Information," in Mark S. Frankel & Albert Teich, The Genetic Frontier: Ethics, Law and Policy. Washington DC: American Association for the Advancement of Science.

Privacy and American Business. 2000. "The IBM-Harris Multi-National Consumer Privacy Survey," Privacy and American Business, 7, 1.

Prosser, William. 1960. "Privacy," California Law Review 48: 383-423.

Raab, Charles D.. 1993. "Data Protection in Britain: Governance and Learning," Governance 6: 43-66.

_____. 1996. "Implementing Data Protection in Britain," International Review of Administrative Sciences 62: 493-512.

_____. 1999. "From Balancing to Steering: New Directions for Data Protection" in Bennett, Colin J. & Grant, Rebecca, eds., Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press.

Raab, Charles D. & Colin J. Bennett. 1994. "Protecting Privacy across Borders: European Policies and Prospects." Public Administration 72: 95-112.

Raab, Charles D. & Bennett, Colin J. 1996. "Taking the Measure of Privacy: Can Data Protection be Evaluated?," International Review of Administrative Sciences, 62: 535-556.

Raines, John Curtis. 1974. Attack on Privacy. Valley Forge, PA: Judson Press.

Regan, Priscilla M. 1981. "Public Uses of Private Information: A Comparison of Personal Information Policies in the United States and Britain." Ph.D., Cornell University.

_____. 1984. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations," Journal of Public Policy 4: 19-38.

_____. 1993. "Ideas of Interests: Privacy in Electronic Communications," Policy Studies Journal 21: 450-469.

_____. 1994. "The Globalization of Privacy: Implications of Recent Changes in Europe," American Journal of Economics and Sociology 52: 257-74.

Regan, Priscilla M. 1995. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press.

Regan, Priscilla M. 1996. "Privacy Legislation in the U.S.: A Debate about Ideas and Interests," International Review of Administrative Sciences 62: 465-478.

_____. 1999. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics" in Bennett, Colin J. & Grant, Rebecca, eds., Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press.

Reidenberg, Joel. M. 1998. "Lex Informatica: The Formulation of Information Policy Rules through Technology," 76 Texas Law Review 76: 553.

_____. 2000. "Resolving Conflicting International Rules in Cyberspace," Stanford Law Review, 52: 1315.

Rosen, Jeffrey. 2000. The Unwanted Gaze: The Destruction of Privacy in America. New York: Random House.

Rosenberg, Jerry M. 1969. The Death of Privacy. New York: Random House.

Rotenberg, Marc. 1991. Privacy Law in the United States: Failing to Make the Grade. Washington D.C.: Computer Professionals for Social Responsibility.

_____. 1994. "Privacy: Political Right or Economic Good," Address given to the 1994 Conference on Computers, Freedom and Privacy (CFP '94), Chicago, March 1994.

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

Rothstein, Mark A., ed. 1997. Genetic Secrets: Protecting Privacy and Confidentiality in the

Genetic Era. New Haven: Yale University Press.

Rule, James B. 1974. Private Lives and Public Surveillance: Social Control in the Computer Age. New York: Schocken Books.

_____. 1996. "Hi-Tech Workplace Surveillance," in Lyon, David & Zureik, Elia, eds., Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Rule, James, Douglas MacAdam, Linda Stearns, and David Uglow. 1980. The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier.

Rule James and Lawrence Hunter. 1999. "Towards a Property Right in Personal Data," in Colin J. Bennett and Rebecca Grant (eds.) Visions of Privacy: Policy Choices for the Digital Age. (Toronto: University of Toronto Press).

Samar, Vincent J. 1991. The Right to Privacy: Gays, Lesbians and the Constitution. Philadelphia: Temple University Press.

Samarajiva, Rohan. 1997. "Interactivity as Though Privacy Mattered," in Agre, Philip E. & Rotenberg, Marc A., eds., Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Schoeman, Ferdinand D. ed. 1984. Philosophical Dimensions of Privacy: An Anthology. Cambridge: Cambridge University Press.

Schwartz, Paul. 1989. "The Computer in German and American Constitutional Law: Towards an American Right of Information Self-Determination," American Journal of Comparative Law 37: 675-701.

_____. 1992. "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," Hastings Law Journal 43: 1321-88.

_____. 1999. "Privacy and Democracy in Cyberspace," Vanderbilt Law Review 52: 1610-1702

_____, and Reidenberg, Joel R. 1996. Data Privacy Law. Charlottesville, Va: Michie

Seipp, David J. 1978. The Right to Privacy in American History. Cambridge: Harvard University Program on Information Resources Policy.

Shils, Edward. 1956. The Torment of Secrecy. Glencoe, Ill: Free Press.

Sieghart, Paul. 1976. Privacy and Computers. London: Latimer.

Simitis, Spiros. 1987. "Reviewing Privacy in an Information Society," University of Pennsylvania Law Review 135: 707-46.

Simitis, Spiros, Ulrich Dammann, Otto Mallmann and Hans Reh. 1981. Kommentar zum Bundesdatenschutzgesetz. 3d ed. Baden-Baden: Nomos.

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

Smith, Janna Malamud and Elizabeth Maguire (eds.) 1997. Private Matters: In Defence of the Personal Life. New York: Perseus Press.

Smith, Robert Ellis. 1979. Privacy: How to Protect What's Left of It. Garden City, NJ: Anchor Press.

_____. 1992. Compilation of State and Federal Privacy Laws. Providence RI: Privacy Journal.

_____. 1993. War Stories: Accounts of Persons Victimized by Invasions of Privacy. Providence RI: Privacy Journal.

_____. 2000. Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. Providence, RI: Privacy Journal.

Sobel, Lester A. ed. War on Privacy. 1976. New York: Facts on File Inc.

Stigler, George J. 1980. "An Introduction to Privacy in Economics and Politics," Journal of Legal Studies 9: 623

Stouffer, Samuel. 1955. Communism, Conformity and Civil Liberties. New York: Doubleday.

Struening, Karen. 1996. "Privacy and Sexuality in a Society Divided Over Moral Culture," Political Research Quarterly 49: 505.

Sullivan, John L., Piereson, James E., & Marcus, George E. 1982. Political Tolerance and American Democracy. Chicago: University of Chicago Press.

Sykes, Charles J. 1999. The End of Privacy. New York: St. Martin's Press.

Taylor, Jim and Wacker, Watts. 1997. The 500 Year Delta: What Happens After What Comes Next. New York: HarperColins.

Thompson, Anthony A. 1970. Big Brother in Britain Today. London: Michael Joseph.

Tilly, Charles ed. 1975. The Formation of National States in Western Europe. Princeton: Princeton University Press.

U.S. Department of Health, Education and Welfare (HEW). Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington D.C.: HEW, 1973.

U.S. Congress. Office of Technology Assessment (OTA), 1982. Computerized Criminal History Systems. Washington D.C.: US Government Printing Office.

_____. 1986. Electronic Record Systems and Individual Privacy. Washington D.C.: US Government Printing Office.

U.S. Privacy Protection Study Commission (PPSC). 1977. Personal Privacy in an Information Society. Washington, D.C.: Government Printing Office.

Van de Donk, Wim. B.H.J. & Van Duivenboden, Hein. 1996. "Privacy as Policy: A Policy Implementation Perspective on Data Protection at Shopfloor Level in the Netherlands," International Review of Administrative Sciences 62: 513-534.

Warner, Malcolm and Michael Stone. 1970. The Data Bank Society: Organizations, Computers, and Social Freedom. London: Allen & Unwin.

Warren, Samuel and Louis Brandeis. 1890. "The Right to Privacy," Harvard Law Review 4: 193-220.

Westin, Alan F. 1965. "Privacy in Western History: From the Age of Pericles to the American Republic." Doctoral Dissertation, Harvard University.

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

_____. 1980. "Introduction," In Donald A. Marchand, The Politics of Privacy, Computers and Criminal Justice Records, Arlington Va: Information Resources Press.

_____, ed. 2000. "The IBM-Harris Multi-National Consumer Privacy Survey," *Privacy and American Business*, 2000, 7: 1

Westin, Alan, ed., & Adams Communications, Co., Ltd., 2000. "Japan Consumer Privacy: A National Survey of the Japanese Public," Hackensack, NJ: Japan-U.S. Privacy and Data Protection Program, Center for Social and Legal Research.

Westin, Alan F. and Baker, Michael. 1972. Databanks in a Free Society: Computers, Record-Keeping, and Privacy. New York: Quadrangle Books.

Whitaker, Reg. 1999. The End of Privacy: How Total Surveillance in Becoming a Reality. New York: W.W. Norton & Company

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

Winner, Langdon. 1977. Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought. Cambridge: MIT Press.