1
The Privacy Paradigm

Introduction

There is plenty of anthropological and sociological evidence that human beings have always needed a degree of privacy. That need is manifested to different degrees and in different ways from culture to culture (Moore 1984, Bok 1982). These questions continue to interest social scientists, for the quest for privacy can tell us a great deal about social relations and structures, now and in the past. However, this book does not address these questions. Instead, we are interested in the processes by which privacy has become a *political* value and a public policy goal, and in what it means to protect privacy when information can flow freely across organizational and jurisdictional borders.

It is first necessary to establish the theoretical tradition from which the contemporary justification for information privacy was derived, and to present the various critiques of this position. Whatever the psychological or sociological evidence for the importance of privacy, the contemporary political justifications overwhelmingly rest on general assumptions about the continued viability of a *liberal* political philosophy and epistemology. We first discuss how those assumptions have been reflected in the privacy literature in different countries. These assumptions entail a number of policy implications. We then review some of the major critiques of the *privacy paradigm* and conclude by suggesting that some of the principal assumptions behind the privacy paradigm require reformulation as a result of some key shifts in the nature and scope of the privacy issue under conditions of globalization.

Privacy and Liberalism

We use the word *paradigm* to denote a set of assumptions about a phenomenon or area of study that generally go unquestioned. These assumptions collectively set the agenda for research and for policy prescription. The paradigm produces an agreed understanding about the nature and scope of a particular problem. Paradigms are rarely explicitly interrogated, unless discoveries in knowledge and science force a community of scholars to confront their long-held and preconceived assumptions (Kuhn 1970). Sometimes that interrogation can occur through the conduct of scientific inquiry; sometimes it can occur because of revolutionary changes in technology. The point is that paradigms are rarely questioned, because for the most part there is no necessity. We would argue that there is a set of unquestioned assumptions that surrounds the modern analysis of privacy protection in Western societies. We also hope to show that these assumptions are in need of careful scrutiny and revision in the light of recent technological developments in the use of personal data in the state and the economy.

The privacy paradigm rests on a conception of society as comprising relatively autonomous *individuals*. It rests on an atomistic conception of society; the community is no more than the sum total of the individuals that make it up. Further, it rests on notions of differences between the privacy claims and interests of different individuals. Individuals, with their liberty, autonomy, rationality, and privacy, are assumed to know their interests, and should be allowed a private sphere untouched by others. In John Stuart Mill's terms, there should be certain "self-regarding" activities of private concern, contrasted with "other-regarding" activities susceptible to community interest and regulation (Mill 1859).

The modern claim to privacy, then, is based 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 of a civil society comprised of relatively autonomous individuals who need a modicum of privacy in order to be able to fulfill the various roles of the citizen in a liberal democratic state. Thus, as Warren and Brandeis comment in their seminal article on the right to privacy: "Still, the protection of society must come mainly through a recognition of the rights of the individual. Each man is responsible for his own acts and omissions only" (Warren and Brandeis 1890, pp. 219–220).

Shils is a twentieth-century proponent of this view that privacy reinforces the barriers between the individual and the state and within the contours of civil society (Shils 1956, pp. 154–160). Privacy, for Shils, is essential for the strength of American pluralistic democracy because it bolsters the boundaries between competing and countervailing centers of power. Westin (1967) has provided perhaps the most eloquent statement of the importance of privacy for liberal democratic societies. 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, p. 24)

Westin goes on to address the specific functions that privacy plays. It promotes 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" (Westin 1967, p. 25). It serves also to shield those institutions, such as the press, that operate to keep government accountable.

Westin also argues that different historical and political traditions among Western nations were likely to create different results in the overall balance between privacy and government. In his view, England 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, pp. 26–27).

Whether or not these generalizations from the 1960s were, or still are, valid, it is no doubt 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 different cultural traditions. The belief in privacy is arguably related to wider attitudes about participation in public affairs and about trust in the authority of governmental agencies. These questions have attracted considerable attention from students of comparative politics (for example, Almond and Verba 1965, 1980), as well as from more anthropological perspectives on social and cultural history (Moore 1984). 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. Much of this argumentation tends, therefore, to invoke anecdotes or cultural stereotypes: "the Englishman's home is his castle," and so on. As we will see in chapter 3, sample surveys on privacy in many countries suggest superficially that populations everywhere have high, and increasing, levels of concern about privacy. These seem mainly to be driven by fears of new technology, and by people's distrust of public and private institutions to use that technology with sufficient respect for the civil liberties of the individual. That distrust may be rooted in different historical experiences, but it appears to be pervasive and strong (Bennett 1992, pp. 37–43).

We would therefore observe that privacy protection is normally justified in individualistic terms in the academic literature and in the popular mind. We each have a right or claim to be able to control information that relates to ourselves. Privacy has an aesthetic and humanistic affinity with individual autonomy and dignity. It can be justified in political terms in that it promotes the institutions of liberal democracy, and it has a number of utilitarian values by way of fostering the principle that "only the right people use the right data for the right purposes" (Sieghart

1976). Whether justified in philosophical, political, or utilitarian terms, privacy is almost always seen as a claim or right of individuals that is threatened by a set of social and technological forces. Privacy is something that "we" once had; now it is something that public and private organizations employing the latest information and communications technologies are denying us.

This paradigmatic theme is represented in a large corpus of polemical literature, written mainly by journalists, activists, and academics. Orwellian metaphors and imagery are naturally prolific, even though 1984 came and went without any palpable change in the attention paid to privacy questions. Among the early examples of the popular American literature are Packard's *The Naked Society* (1964) and Brenton's *The Privacy Invaders* (1964). Continually over the past thirty years or more, publishers in North America,[1] Britain,[2] and elsewhere have been attracted by this more polemical genre. The literature also encompasses a shifting anxiety over emerging technologies. This ranges from apprehension over the "snooping devices" of the 1960s, to worries about the sophisticated trade in personal information revealed in Rothfeder's *Privacy for Sale* (1992), to the more contemporary concerns about the Internet discussed by Diffie and Landau (1998) and by Garfinkel (2000), or about the excessive responses to 9/11 (Rosen 2004).

The importance of this literature arguably 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). Moreover, many of these stories have then been picked up by the print and visual media, especially television. 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; they also make good films.[3]

The contexts may change, the technologies may evolve, but the message of this genre is essentially the same: privacy is eroding, dying, vanishing, receding, and so on. Despite privacy laws, conventions, codes, oversight agencies, and international agreements, privacy (as typically

defined) is something of the past, to the extent that a prestigious magazine can proclaim in an editorial (The *Economist* 1999, p. 16): "Privacy is doomed . . . get used to it."[4]

Policy Implications of the Privacy Paradigm

The pervasiveness of liberal assumptions within the literature has had a number of political and policy implications. Assuming that we each have privacy rights and interests, how can one frame a public policy to protect those rights? Philosophers, academic lawyers and other scholars have debated the meaning of *privacy* from a variety of standpoints (for example, Young 1978, Schoeman 1984). As a policy problem, however, the discourse settled around *information privacy*, a concept that arose in the 1960s and 1970s at about the same time that *data protection*, derived from the German *Datenschutz*, entered the vocabulary.

Concerns obviously differed among a number of advanced industrial states. However, a closely knit group of experts in different countries coalesced, shared ideas, and generated a general consensus about the best way to solve the problem of protecting the privacy of personal information (Bennett 1992, pp. 127–129). The overall policy goal in every country was to give individuals greater control of the information that is collected, stored, processed, and disseminated about them by public and, in some cases, private organizations. Essentially, the common view was that this goal necessitates a distinction between the *subject* of the information and the *controller* of that information. This distinction is one of role rather than of person: although we are all "data subjects," many of us are also "data controllers" or "data users." By the 1980s, therefore, it is possible to discern the set of key assumptions upon which information privacy policy development rested.

The first assumption was that privacy is a highly subjective value. Concerns about the protection of personal information vary over time, across jurisdictions, by different ethnic subgroups, by gender, and so on. Consequently, public policy cannot second-guess the kinds of personal information about which a given population or group will be concerned at a given time. Public policy and law can only establish the

rules, principles, and procedures by which any individually identifiable personal information should be treated, and by which the worst effects of new technologies can be countered. Information privacy policy is based inevitably, therefore, on *procedural*, rather than *substantive*, tenets. It can put in place the mechanisms by which individuals can assert their own privacy interests and claims, *if they so wish*, and it can impose obligations on those who use personal data. But for the most part, the content of privacy rights and interests have to be defined by individuals themselves according to context.

It is generally difficult to define a priori those data that are inherently worthy of greater protection ("sensitive data"). It is often the shift of context—detaching personal data, through processing, from the circumstances of their original collection—rather than the properties of the data that lead to privacy risks when false conclusions are drawn about persons (Simitis 1987, p. 718). In addition, the same information can take on very different sensitivity levels in different contexts. Our names in the telephone directory may be insensitive; our names on a list of bad credit risks or of sex offenders may be very sensitive. A name and address in a telephone directory may be insensitive for most people, but may be very sensitive for vulnerable persons who do not want to be monitored and tracked down. Whereas the name "P. J. O'Reilly" is not particularly conspicuous in the telephone directory of an Irish town, it stands out in the telephone directory of a Chinese town. Little wonder that many people prefer to have unlisted telephone numbers. Examples of such people would be battered wives, doctors who perform abortions, celebrities, child protection staff, police officers, and so on.

For the most part, therefore, public policy cannot draw a definite line between those types of information that should remain private, and those that may be in the public domain. Law cannot easily delineate between those types of data that are particularly worthy of protection and those that are not. Some data protection laws have indeed distinguished between what are generally agreed to be sensitive data—religious beliefs, political opinions, sexual preferences, health, and the like—and the rest. But this distinction, and the inventory of data deemed sensitive, has remained controversial.

A second conclusion stemmed from the observation that personal information cannot easily be regarded as a property right. Classic economic theorizing would contend that an imperfect marketplace can be rectified in one of two ways. First, one can give a value to personal information so that the costs and benefits of transactions are allocated more appropriately. But it is very difficult to establish personal information as property in law, and then to define rights of action over its illegitimate processing. Consumers may have some bargaining power with a direct marketing firm that wants to trade lists of named individuals; citizens, however, have no bargaining power when faced with a warrant or any other potentially privacy-invasive technique backed by the sanctions of the state. Let us recall that, at the outset of the privacy debate, it was the power of government agencies that were considered to pose the most significant challenges. It was therefore hard to resist the conclusion that the imbalance could only be set right by regulatory intervention. Consequently, information privacy was generally defined as a problem for public policy, rather than as an issue for private choice.

More recently, as critiques of the dominant approach have surfaced, the personal data processing practices of the private sector have arisen as equally significant concerns. Moreover, as Internet communications and e-commerce have risen to prominence, so a variety of market-based solutions have been proposed, all of which have been based on the premise that personal information can be given a property value, to be traded and exchanged within the personal information market (Laudon 1996, Rule and Hunter 1999, Lessig 1999). Such arguments had, however, very little influence on the experts and legislators that grappled with the information privacy problem in the 1970s.

A third assumption concerned the relationship between information privacy and information security. These and related concepts (data protection, data security, confidentiality, etc.) have caused considerable confusion. Clarke notes:

> The term "privacy" is used by some people, particularly security specialists and computer scientists, and especially in the United States, to refer to the security of data against various risks, such as the risks of data being accessed or modified by unauthorised persons. In some cases, it is used even more restrictively, to refer only to the security of data during transmission. These aspects are only a small fraction of the considerations within the field of "information privacy." More appropriate terms to use for those concepts are "data security" and "data transmission security." (Clarke 1999, p. 3)

In other words, data security is a necessary but not a sufficient condition for information privacy. An organization might keep the personal information it collects highly secure, but if it should not be collecting that information in the first place, the individual's information privacy rights are clearly violated. Over time, it became clear that the European concept of *data protection* was being used in much the same way as the term *information privacy*. Some, however, see this term as overly technical and concentrating on the *data* rather than the *person* as the object of protection.

Finally, there has been a consensus that the focus of protection should be the individual, or the "natural person" rather than some other entity. Therefore, organizations and corporations cannot have privacy rights. Some societies—in Scandinavia, for example—have attempted to embrace the rights of natural and legal persons in their data protection legislation, and Westin himself was certainly open to the possibility that groups and organizations could have privacy "claims" (Westin 1967, p. 7). Nevertheless, information privacy policy did develop, domestically and internationally, on the assumption that the interests of groups, corporations, and other organizations and the information about them can and should be dealt with through other legal instruments.

These assumptions might not be accepted by every scholar and commentator. They were and are deeply contested. The basic point at this juncture in the analysis is that privacy protection policy was set on a particular trajectory as a result of some common assumptions about the nature of the information privacy problem. It is particularly noteworthy that the privacy paradigm is not only shared by intellectuals and popular commentators, but also by those who make and implement privacy protection policy in advanced industrial states. The policy responses that developed—data protection or information privacy statutes—were driven for the most part by a shared understanding among policy elites about the nature of the problem they were facing. Those shared assumptions, based on fundamental liberal principles, have had profound and widespread policy implications in every advanced industrial state.

The "Fair Information Principles" Doctrine

From these realizations flows the doctrine of "fair information principles" (FIPs), enjoining upon data controllers norms for the collection, retention, use, and disclosure of personal information. The codification of these principles has varied over time and space. They appear either explicitly or implicitly within all national data protection laws, including those that, in the United States, Australia, New Zealand, and Canada, are called Privacy Acts. They appear in more voluntary codes and standards (for example, CSA 1996). They also form the basis of international agreements, which will be discussed in chapter 4. These include the 1981 *Guidelines* of the Organization for Economic Cooperation and Development (OECD 1981), the 1981 *Convention* of the Council of Europe (CoE 1981), and the *Directive on Data Protection* of the European Union (EU 1995). Over time, there has emerged a strong consensus on what it means for the responsible organization to pursue fair information practices responsibly.

While the codification of the principles may vary, they essentially boil down to the following tenets (Bennett and Grant 1999, p. 6). An organization (public or private)

- must be *accountable* for all the personal information in its possession;
- should *identify the purposes* for which the information is processed at or before the time of collection;
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality* principle);
- should *retain* information only as long as necessary;
- should ensure that personal information is kept *accurate, complete, and up-to-date*;
- should protect personal information with appropriate *security safeguards*;

- should be *open* about its policies and practices and maintain no secret information system;
- should allow data subjects *access* to their personal information, with an ability to amend it if it is inaccurate, incomplete, or obsolete.

These principles are, of course, relative. However conceptualized, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community, and can be overridden by other important values and rights. Hixson (1987) 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, pp. xv–xvi). An assumption of balance underlies many of the official investigations into privacy policy. The US 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" (PPSC 1977, p. xv).

However, this concept is problematic both as a verb and a noun (Raab 1999a). It does not discriminate between divergent conceptions of what it means, in practice, *to balance*; nor does it provide criteria for judging when a balance has been achieved. It is therefore not very informative to hear that "a balance must be struck between privacy and the public interest," or that "we have found the right balance" between the one and the other. Different people may go about finding a balance in different ways, and arrive at different substantive points of reconciliation between competing values, as we shall see shortly. Although the concept is related to the terminology of judicial decision, the achievement of a balance may ultimately be a matter of political negotiation, perhaps arriving at a consensus; or, alternatively, of authoritative assertion.

There are, however, many cross-national divergences in the content of privacy protection policy. Privacy regimes, discussed in chapter 8, involve a number of different participants who may play subtly different roles depending on the jurisdiction within which they exist and the political factors that have shaped these regimes. Moreover, not all

advanced industrial states have accepted the logic behind privacy protection policy for every kind of personal data controller; the private sector is still largely unregulated in the United States, for example.

Critiques of the Privacy Paradigm

Not all commentators have accepted the logic outlined above. From the outset of the modern debate, there has been a lively but often marginalized critique of liberal political theory as a basis for privacy. This critique has come from at least four overlapping theoretical positions. First, some skeptics have noted that there is a definite negative dimension to the notion of privacy as the "right to be left alone." On the one hand, it draws attention to why one might want to be left alone, and invites the criticism that privacy rights are predominantly asserted by those who have the most to hide. Here is a quote from an early article by Arndt (1949): "The cult of privacy seems specifically designed as a defence mechanism for the protection of anti-social behaviour." He equates 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, p. 70).

A similar critique of the theory of information privacy was presented in a famous article by Posner (1978). Posner's central point is that the application of the principle of information privacy has an unfortunate corollary, namely that it allows people to conceal personal information in order to mislead and misrepresent their character. Others, including government institutions, "have a legitimate interest in unmasking the misrepresentation." "It is no answer," he continues, "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 1978, p. 20).

A second line of attack has come from those who find the distinction between public and private problematic. They cannot be treated as separate entities but are complex concepts that operate on different dimensions according to whether one is analyzing access to information, the capacities in which agents enjoy that access, or in whose interest the access is sought.

By extension, feminists have criticized privacy 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, Boling 1996). Allen and Mack (1990) criticize Warren and Brandeis on these grounds: 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 decision-making 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 and Mack 1990, p. 477).

Thirdly, and 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. Pateman (1970), for example, has contended that there are two general traditions of democratic theory. One is a liberal tradition rooted in eighteenth 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, nor 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."

This argument finds current reflection in the renewed interest in the communitarian theorizing of Etzioni (1999), which has resonated with contemporary political elites of the left and the right in both Europe and America. Etzioni explicitly attempts to point to a new "communitarian concept of privacy"—"one that systematically provides for a balance between rights and the common good" (Etzioni 1999, p. 15). His analysis of privacy builds on "the sociological observation that although ideologies can be structured around a single organizing

principle—like liberty, or a particular social virtue—societies must balance values that are not fully compatible" (Etzioni 1999, p. 200). He contends that, insofar as the public sector is concerned, the balance is too often struck in favor of privacy, while private sector abuses often go unchallenged.

A communitarian position might even argue that some of the most creative civilizations in history—such as ancient Greece and Rome, and Renaissance Italy—flourished despite, or maybe because of, the lack of individual privacy. Public philosophies, including communitarianism, do not spring from an emphasis on the "right to be let alone." If information privacy, as it is conventionally construed, is a precondition of democracy, it is not of democracy per se but of a particular form—liberal democracy, the theoretical justifications for which were provided by Locke, Madison, and Mill, rather than by Jean-Jacques Rousseau. However, there are alternative ways of looking at privacy, and these can serve other notions of democracy. We touch upon this again in the conclusion to this chapter, and develop it at greater length in chapter 2.

A final, and more recent, critique emerges from those who argue from poststructuralist assumptions that the essential ontological premise about the central autonomy of the subject is misguided. In explicating Foucault's (1979) notion of the "panopticon," as a new form of everyday surveillance and social control, Poster explains the postmodern and poststructuralist 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 that "real" self ever being aware of what is happening. (Poster 1990, pp. 97–98)

Poster's (1990) 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. As Lyon puts it, 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, p. 18). We take up this thread in the next section.

Thus the privacy debate has sometimes raised some insightful and controversial theorization about the concepts *public* and *private* and has echoed some of the claims and counterclaims within political theory generally. For the most part, however, political theorization about privacy has operated within the basic liberal paradigm. The privacy literature has assumed a distinction between the realms of the public business of the state, and the private spheres of individual life. It has also remained relatively unaffected by deeper questions about cultural relativity, or bias according to class, gender, race, or other social categories.

To some extent, this is explained by the fact that much of the more philosophical debate about privacy has originated in or 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. The bulk of the more abstract and conceptual literature was prompted by the need to understand the emerging "right to privacy" that the US Supreme Court was in the process of developing and applying to private decisions about intimate family concerns such as contraception and abortion. In the tradition of Warren and Brandeis (1890), much of the philosophy of privacy is, therefore, understandably directed towards emerging legal doctrine (for example, Prosser 1960, Fried 1968, Parker 1974, Gavison 1980, Parent 1983). It has remained relatively untroubled by deeper questions about the nature of the *self* in modern or postmodern conditions. The political theory of privacy, in both the United States and Europe, has largely operated within a liberal paradigm and has not yet confronted more profound ontological, epistemological, and sociological issues. The links between the vast tradition of political theory, including its rich and multifaceted critique of the many varieties of liberalism, and the theoretical and practical literature on privacy are, therefore, tenuous.

Surveillance and the Collective Threat to Individual Privacy

As we have just mentioned, 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, they claim, the problem is *surveillance*, or excessive and illegitimate surveillance. Thus a sociological tradition has attempted to equate the loss of privacy with some deeper forces associated with modern or postmodern life. Underlying much of the sociological literature is the Foucauldian concept of "panopticism" as a phenomenon that operates as a process of disciplinary classification and control (see Gandy 1993, pp. 3–13).

"Rather late in the day," Lyon argues (1994, p. 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." The argument that the institutions of surveillance constitute a theme within modernity, separate from industrialism, capitalism, and the control of the means of violence, is principally associated with the writings of Giddens (1991), who says that each of these forces can be "distinguished analytically from the institutions of surveillance, the basis of the massive increase in organisational power associated with the emergence of modern social life" (Giddens 1991, p. 15). But, for Giddens, surveillance always operates in conjunction with what he terms "institutional reflexivity," the continual need to monitor what is going on, which becomes a constitutive element in an institution's identity and self-reference. Thus, "[s]urveillance plus reflexivity means a 'smoothing of the rough edges' such that behavior which is not integrated into a system . . . becomes alien and discrete" (Giddens 1991, p. 150).[5]

Within political science, the analysis of surveillance has 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 individual behavior within Stalinist and Fascist systems (Westin 1967). To a certain degree, and perhaps particularly in Europe, the interest in privacy among scholars was motivated by a desire to build institutional and cultural barriers

against the comprehensive monitoring of private life that appeared—before the Second World War and during the Cold War years—as a necessary condition for the functioning of totalitarian or authoritarian regimes. Only in post–Cold War times has the pervasiveness of secret-police surveillance in Eastern and Central Europe come into clearer focus through the dismantling of state-security institutions in several countries, and through the accounts of writers like Ash (1997).

In liberal democratic states, however, rather different questions have been raised about the insidious growth of sometimes more subtle forms of surveillance. 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? Or is it more rooted in the demands of the capitalist mode of production, and in the responses of even liberal states to threats to national security? Maybe all of these. Perhaps Foucault's point, reflected in Lyon (2001), 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, albeit perhaps too sweeping as an explanation.

From the perspective of those social scientists 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 for excessive intrusions. Thus privacy and data protection laws can only have a marginal impact on the development of surveillance societies; some even would contend that they serve to legitimize new personal information systems and thus extend social control.

A formidable critique of the liberal theory of information privacy is given by Rule and his colleagues (1980). They claim that privacy and data protection laws are all well and good, but that 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. On the contrary, there are persuasive cases of the enactment of data protection law being used to legitimate the introduction of new surveillance systems. The essential problem for Rule, then, is the inherent tendency of bureaucratic organizations to want to collect and store more and more increasingly detailed personal information. This dynamic of complex organizations has its roots in the eighteenth century, and in the move towards rationalization and control of resources that accompanied industrialization (Beniger 1986). 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 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. Flaherty, a Canadian scholar of legal history and subsequently Information and Privacy Commissioner of British Columbia, gave the title of *Protecting Privacy in Surveillance Societies* to his comparative analysis of the operation of data protection laws (Flaherty 1989). He begins: "The central theme of this volume is that individuals in the Western world are increasingly subject to surveillance through the use of data bases 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" (Flaherty 1989, p. 1). Flaherty demonstrates how countries that have established data protection agencies, including 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. Echoing Rule's analysis, he suggests that "[a]t 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" (Flaherty 1989, p. 384).

As technological tools became smaller, less expensive, and more decentralized during the 1980s, other analysts have stressed rather different aspects of the problem. Marx's (1988) study of undercover police surveillance is a case in point. He demonstrates how incremental changes in technology, social values, and the law encouraged covert and deceptive police techniques with a variety of intended and unintended consequences. He shows 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.[6] "The awesome power of the new surveillance," Marx summarizes, "lies partly in the paradoxical, never-before-possible combination of decentralized and centralized forms" (1988, pp. 217–219). This analysis led him, in more recent writing, to propose a completely revised "ethics for the new surveillance" to replace what he regards as the outmoded and limiting "fair information principles" doctrine (Marx 1999).

Two other writers who have directed their attention as much to private as to public sector practices see other trends at work. Gandy (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 in both sectors. He points out that a number of social theorists (Karl Marx, Ellul, Giddens, Weber, Foucault) 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: "[t]he 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" (Gandy 1993, p. 15). Gandy's analysis leads him to the conclusion that real consumer choice can only be implemented through "opt-in" (positive consent) rather than "opt-out" (negative consent) provisions.

Lyon (1994) employs more visual imagery to address similar questions about surveillance. Drawing inspiration from much the same literature as does Gandy, he too contends that surveillance cannot be reduced to one social or political process. But whereas Gandy relies on contemporary empirical analysis of the surveillance practices of modern corporate and bureaucratic organizations, Lyon adopts a more historical approach. He links surveillance to theories of modernity, and speculates on the possibilities and implications of a more communitarian postmodern 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 (Lyon 2001, pp. 53, 136–137).

The arguments of those who stress information privacy, and those who stress surveillance, have often been posited as diametrically opposed political stances. However, the distinction should not be exaggerated. The difference stems more from the starting-point: whether it is from the erosion of privacy and how the institutions of a liberal society might cope with the most dangerous and intrusive threats from new technologies, or whether it is from an interest in the changing impact and nature of social control and disciplinary practice. The processing of personal data by private and public institutions is, from this latter perspective, a way to shed light upon broader social and technological trends.

The privacy and surveillance literatures can often be regarded as two sides of the same coin. With few exceptions, most of the literature we have reviewed would share the following four assumptions:

- that privacy is an individual right;
- that privacy is something that we once had and is now eroding;
- that the source of the privacy problem is structural—the set of impersonal and remote forces that together contribute to the declining ability of individual agents to control the circulation of information that relates to them; and
- that the organizations that are responsible for privacy invasion can be observed, resisted, and regulated because they are subject to a set of obligations that stem from principles as embodied in the laws of discrete and bounded liberal democratic states.

In the conclusion to this chapter, we raise questions about each of these assumptions.

Conclusion: Privacy and the Liberal Democratic State

The privacy paradigm, based on a conceptualization of distinct private and public realms, almost inevitably leads the debate to a discussion of how privacy conflicts with social or community values; this debate is prompted, for example, by the first assumption that we have identified. It often leads to the view that privacy and social values such as sociability, internal security, social welfare, or government efficiency are necessarily antithetical. The problem here is not only the deeply contested and ambiguous quality of these concepts, but also that the promotion of privacy can itself be socially important.

Regan (1995) has gone far to develop the theory of privacy as a value for entities beyond the person. 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. (Regan 1995, p. 221)

Regan makes the important point that "[p]rivacy is becoming less an attribute of individuals and records and more an attribute of social relationships and information systems or communication systems" (Regan 1995, p. 230). In this sense, it can be argued that excessive surveillance is bad not only for individuals, but also for society. Take a contemporary example: video-surveillance cameras (CCTV) in public places can be justified as a necessary remedy to deter and detect crime. On an individual level, they can be criticized as being overly intrusive, and may lead to mistaken identification with adverse consequences. On a societal level, we might properly question whether, as a society, we wish to go about our daily affairs with cameras recording our every movement, and enabling the compilation of comprehensive records of what we do, with whom, when, and where.

Moreover, such surveillance may have a chilling effect on associational activity, to the detriment of society. This argument is made in a

similar critique by Schwartz (1999), who elaborates a theory of "constitutive privacy" to replace "the traditional liberal understanding of information privacy, which views privacy as a right to control the use of one's personal data" (Schwartz 1999, p. 1613). In analyzing a variety of recent practices on the Internet, Schwartz is persuaded that the silent collection of personal information in cyberspace "has a negative impact on individual self-determination; it makes it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends" (Schwartz 1999, p. 1701). As we saw, Westin's (1967) account of privacy also highlights certain political values, including freedom of association and the secret ballot. Among his "four states of privacy" (Westin 1967, pp. 31–32), intimacy and anonymity imply the ability of individuals to engage others, rather than signifying their withdrawal from society. These two "states" therefore sustain participation in collective political life, including such modes of activity as associating politically with others or voting without the fear of surveillance.

As seen in analyses such as these, this relationship between privacy and political participation opens an avenue, even within the conventional paradigm, for considering privacy as a value for society beyond the single individual or beyond a simple aggregate of individuals. In a related fashion, we argue that excessive surveillance can lead to the erosion of trust, that it can exacerbate risk, and that it can lead to social inequities. Each of these values (equity, trust, and risk) can be promoted when privacy protection is viewed as social policy. In chapter 2 we elaborate Regan's (1995) argument and investigate how privacy protection policies can promote equity; we consider the reduction of risk and the promotion of trust in chapter 3.

The second of the four assumptions is that our privacy is eroding, vanishing, diminishing, and so on. We question such fatalism from a number of perspectives. We simply do not know whether we would have enjoyed higher "levels" of privacy in the past. How does one calibrate a "level" of privacy? Who are "we"? These measurements are surely highly subjective and dependent on a range of diverse contextual circumstances, as we will touch on in chapter 9. The mediaeval village and nineteenth-century industrial town were not particularly privacy-

friendly places. The argument about the erosion of privacy depends on the starting-point. Typically, the fatalistic contention means that organizations simply know more about our lives than they did in the past. If one were to reckon the sum total of information that external structures "know" about us, that aggregation would be far greater than it would be for our predecessors who lived and worked in feudal and industrial societies. We therefore have less control over the amount and quality of the information that relates to us. Stated in this fashion, the problem becomes less one of stemming the collection of information, and more one of ensuring its appropriate use and disclosure. To the extent that this is so, the problem is inherently about social relations and their management.

Thirdly, therefore, the privacy value relates to more than the loss of human agency in the face of impersonal structural forces, whether bureaucracy, capitalism, or technology. We would insist that the privacy problem has its roots in human agency as well as in structural conditions: "[p]rivacy problems arise when technologies work perfectly and when they fail. They arise when administrative, political, and economic elites have worthy motives, and when they do not. They arise through both human fallibility and infallibility" (Bennett and Grant 1999, p. 4).

The scope of the privacy issue can be heuristically demonstrated through a four-cell matrix as depicted in figure 1.1. One axis displays

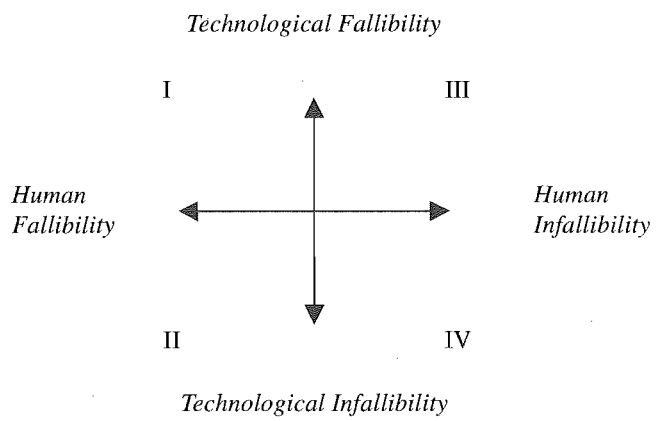

Figure 1.1.
A matrix of privacy problem sources

a difference in the fallibility of human agents; the other shows a difference in the fallibility of structures, which might be technological or organizational. Our point is that "privacy problems" can occur within each cell of the framework. Because each axis is a continuum, positions may be found in any part of each cell. We think, however, that in practice most positions will be found nearer the crossing than the extreme corners in each cell: few human agents, and few technical systems, are either perfect or imperfect.

Most privacy-related problems tend to be seen where human fallibility combines with technological fallibility (I): excessive collection of personal data, inaccuracies, inappropriate disclosures, and so on. To reverse Sieghart's (1976) formula, problems arise when the "wrong data are used by the wrong people for the wrong purposes." The long-held concern about a "Chernobyl" for privacy is also premised on an assumption of human and technological fallibility. But where technologies and humans combine perfectly to pursue organizational goals (IV), there is not necessarily a concomitant lowering of the risk to privacy. Indeed, the fear of the "surveillance society" in which our personal data can be matched, profiled, mined, warehoused, and manipulated for a range of social and economic ends is premised exactly on the fear that human agents and new technologies will combine *as intended* to reach new levels of intrusiveness, and from which there is no escape. Examples of this are the often surreptitious extraction and processing of personal data on Internet websites, and the sharing of personal data by government agencies to provide a range of services to the citizen. Of course, the "infallibility" of these systems may only be an aspiration that is never fully achieved in practice.

On occasion, the quality of human performance can be very high, but the technologies may fail (III); for instance, databases may be obsolete or highly inaccurate, or data-processing capacity may be deficient, or computer systems may be vulnerable to a variety of malicious attacks. On the other hand, technologies may perform as intended, while human agents err (II): they may draw the wrong inferences or conclusions from outputs of data produced by the system, whether because of inadequate training, the biases inherent in the pursuit of certain organizational goals, the pressures of reward systems in the organization, or some other reason related to the workings of human agency.

This simple framework, which could obviously be made more complex, is offered to counter the position that privacy-related risks stem from only one source. Their complexity may have increased as a result of the use of high technology in complex organizations. But they may just as easily relate to human fallibility—a perennial condition that can cause paper medical records to appear on rubbish tips, or damaging faults to appear in the most sophisticated computer program. Thus, the picture of an embattled individual trying to stem the tide of surveillance flowing from a range of impersonal and invulnerable structural forces makes good rhetoric for the privacy cause, but it distorts reality and oversimplifies social and political analysis.

Finally, and relating to the fourth underlying assumption about the role of the state, we wish to investigate the implications for privacy analysis and policy prescription when personal information knows neither organizational nor national attachments. The privacy paradigm, like liberalism, tends to be state-centric. We mean this in two different senses. First, the right to privacy is generally regarded as a benefit of state citizenship. These rights are conferred on us by virtue of our identities as Americans, Britons, Canadians, Germans, or whoever. The privacy and data protection laws that provide us with certain guarantees about our personal information reflect some essential principles of liberal democracy that are either enshrined in constitutions (such as the US Fourth Amendment) or are deeply embedded in the cultural and historical experiences of different societies.

Second, there is still an assumption that the primary threat to these rights emanates from within the state in which one is living, stemming from practices occurring within the boundaries of discrete states, whether in public agencies or in the private sector. This view was prevalent twenty years ago, when many of the European data protection laws were being promulgated, but contemporary discourse and policy prescriptions are still generally dictated by a paradigm that suggests that our personal information still tends to be held within organizations that are easily identifiable, stable, and that reside and operate within the

boundaries of modern territorial states. However, many scholars, inspired by various themes prevalent in the literature on postmodernity, have questioned the empirical and theoretical reliance on the state for policy prescriptions in a range of policy sectors—the environment, consumer protection, taxation, and so on. We raise similar questions with respect to privacy protection. Information and communication technologies, systems, and practices involving personal data have changed dramatically over the past twenty years or so. When the problem is increasingly unbounded by state borders, how has this problem been redefined? What are the new policy instruments that have arisen? And what are the prospects for promoting this essential value within a globalized economy?

2

Privacy Protection as Social Policy

Introduction

In chapter 1 we signaled our argument that excessive surveillance can lead to social inequities. This statement has meaning only to the extent that comparisons can be made among individuals in terms of their relative enjoyment of privacy as a value. Looking at privacy in this way does not deny its abstract quality as a right, or even as a preference. However, it allows us to consider privacy issues beyond the conventional paradigm. That paradigm comprehends the individual's privacy and its protection almost completely in terms of individual rights or choices, as if protecting the exercise of one's right to, or choice of, a "level" of privacy could be the only objective of public policy. Yet, even to the extent that privacy *is* a value for individuals to enjoy, it would still be relevant to ascertain who enjoys what privacy, and why. This is because the extent to which individual values are, or can be, satisfied is influenced by social, economic, and political factors beyond individuals themselves, which can be shaped by evidence-based public policy. These factors have distributive consequences for individuals, and thus for society as a whole.

The knowledge basis for informing privacy policy is underdeveloped, and seems to be further advanced for information policy more generally. In academic circles, the economic and social implications of the "information revolution" are being analyzed and projected in considerable detail (Castells 1996, Dutton 1996, 1999, Shapiro 1999, Lessig 1999). Although a long-neglected issue, this analysis now includes investigation of the question of unequal access to the benefits of the "information