Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 431–453

Social and Political Dimensions of Privacy

Alan F. Westin*
Columbia University

This article provides a framework for analyzing privacy in modern societies, defining information privacy and describing three levels that structure the values assigned to privacy. After describing a contemporary privacy baseline (1945–1960), these concepts are applied to social and political privacy developments in three contemporary eras of steadily growing privacy concerns and societal responses across citizen-government, employee-employer, and consumer-business relationships in 1961–1979, 1980–1989, and 1990–2002. Each period is described in terms of new technology applications, changing social climates, and organizational and legal developments. Effects of the 9/11 terrorist attacks on privacy balances are analyzed and predictions for future privacy developments are presented. The relationship of articles in this issue to the author's framework is noted throughout.

A Conceptual Framework for Information Privacy Analysis

I have defined privacy as the claim of an individual to determine what information about himself or herself should be known to others (Westin, 1967, Part One. See also Bennett, in preparation; Pennock & Chapman, 1971; Solove, 2002). This, also, involves when such information will be obtained and what uses will be made of it by others. I add a claim to privacy by social groups and associations, and also a limited (largely temporary) right of privacy for government processes. When a privacy claim is recognized in law or social convention, we can speak of "privacy rights." To examine how privacy norms operate in any society, we need to track

*Correspondence concerning this article should be addressed to Alan F. Westin, President, Center for Social and Legal Research, Suite 414, Two University Plaza, Hackensack, N.J. 07601 [e-mail: alanrp@aol.com].

This article draws for its opening sections and at other points on my 1967 book, *Privacy and Freedom*, and the manuscript of a forthcoming volume I have edited, tentatively titled: Privacy and Freedom *Updated: Social Science Perspectives on Privacy*.

three settings: The political, the socio-cultural, and the personal (the following discussion is drawn from Westin, 1967, Part One, 1991, and in preparation, and sources there cited).

Privacy at the Political Level

Every society sets a distinctive balance between the private sphere and the public order, based on the society's political philosophy. In this issue, the Culnan and Bies (this issue), Margulis (this issue, "Privacy as a Social Issue"), Marx (this issue), and Regan (this issue) articles explore aspects of this dimension. In broad terms, privacy norms are set in two alternative societal models, in authoritarian and democratic societies. (see Westin, 1967, Chap. 2).

Though democratic societies value and institutionalize privacy, democracies must also provide for the disclosure of information necessary to the rational and responsible conduct of public affairs and to support fair dealing in business affairs. Officials must engage in surveillance of properly identified anti-social activity to control illegal or violent acts. In addition, the urges of curiosity and gossip in society compete with privacy claims; recent trends such as intrusive mass media and contemporary confessional television can generate strong voyeuristic threats to privacy. Managing this tension among privacy, disclosure, and surveillance in a way that preserves civility and democracy, and copes successfully with changing social values, technologies, and economic conditions, is the central challenge of contemporary privacy definition and protection (Westin, 1967, Chap. 3).

Privacy at the Socio-Cultural and Organizational Level

The political balance is the framework for a second level of privacy—the socio-cultural and organizational level (Westin, 1967, Part One, and sources there cited). In this issue, Alpert (this issue), Culnan and Bies (this issue), Gandy (this issue), Margulis (this issue, "On the Status"), Marx (this issue), and Stone, Stone-Romero, and Hyatt (this issue) explore these dimensions.

At the socio-cultural level, environmental factors such as crowded cities and class factors of wealth and race shape the real opportunities people have to claim freedom from the observation of others (Geller, in preparation; Westin, 1967). In this sense, privacy is frequently determined by the individual's power and social status. The rich can withdraw from society when they wish; the lower classes cannot. The affluent do not need to obtain subsidizing support from the government by revealing sensitive information to authorities, while those in economic or social need must disclose or go without. Ironically, though, the rich, the famous, and the politically powerful are also the people whose privacy is most assaulted by the media, political rivals, government investigators, and the like. And, in an age of virtually universal record-keeping and credentials review, even the wealthy and

powerful become enmeshed in all-pervasive data-collection processes (Rule, 1973; Wheeler, 1969).

At the socio-cultural level, privacy is closely related to social legitimacy (Geller, in preparation; Westin & Baker, 1972). When a society considers a given mode of personal behavior to be socially acceptable—whether it is hairstyle, dress, sexual orientation, political or religious belief, having an abortion, or other lifestyle choice—it labels such conduct as a private rather than a public matter. This generally means that such matters should not be inquired into for the purpose of denying someone access to the benefits, rights, and opportunities controlled by government or private organizations.

When society does not accept certain personal conduct, it is saying this is not a matter of private choice and does not allow a claim of privacy. Thus, debates over privacy are never-ending, for they are tied to changes in the norms of society as to what kinds of personal conduct are regarded as beneficial, neutral, or harmful to the public good. In short, privacy is an arena of democratic politics. It involves the proper roles of government, the degree of privacy to afford sectors such as business, science, education, and the professions, and the role of privacy claims in struggles over rights, such as equality, due process, and consumerism.

Individual Privacy: Four Basic States and Their Self-Management

Finally, within the political and socio-cultural limits just described, claims of privacy are asserted by each individual in daily life, as he or she seeks an intrapsychic balance between privacy and needs for disclosure and communication (Regenold, in preparation; Westin, 1967; and sources there cited). In this issue, DePaulo, Wetzel, Sternglanz, and Walker Wilson (this issue) and Margulis (this issue, "On the Status") assess these aspects. Individual privacy balances are a function of one's family life, education, social class, and psychological makeup. This dimension of privacy reflects each individual's particular needs and desires and will shift constantly in terms of life-cycle progress and situational events. I have identified four psychological conditions or states of individual privacy—solitude, intimacy, anonymity, and reserve. These are fully discussed in Westin (1967) and in Margulis (this issue, "On the Status"), and my 1967 formulations are updated in Westin (in preparation).

In these states of privacy, the individual's needs are constantly changing. At one moment, a person may want to be completely alone, in down time. At another moment, individuals may want (or even desperately need) the companionship or sustaining presence of an intimate friend. Or, the individual may want to open up problems or situations to a complete stranger—the one-time acquaintance who will listen to the individual's problems but who will not be encountered again and will not exercise judgmental authority over the individual (Westin, 1967, Part One).

Such changing personal needs and choices about self-revelation are what make privacy such a complex condition, and a matter of personal choice. The importance of that right to choose, both to the individual's self-development and to the exercise of responsible citizenship, makes the claim to privacy a fundamental part of civil liberty in democratic society. If we are switched on without our knowledge or consent, we have, in very concrete terms, lost our rights to decide when and with whom we speak, publish, worship, and associate. Privacy is therefore a social good in democratic societies, requiring continuous support from the enlightened public (Regan, 1995; Westin, 1967, Part Four).

Contemporary Stages of Privacy Development

After describing a Privacy Baseline (1945–1960), I posit three phases of contemporary privacy development: 1961–1979, 1980–1989, and 1990–2002. In each, I describe changes in three factors that drive privacy developments: new technologies and their applications by organizations, social climate and public attitudes, and organizational policies and law. In addition, there are three sets of relationships between individuals and authorities that usually call for differentiated treatment—citizen-government, consumer-business, and employee-employer. Each has different power relationships, prevailing expectations, and legal frameworks.

Interest-Group and Ideological Positions

I see privacy politics also featuring a continuing conflict among three interest-group and ideological orientations. A high-privacy position assigns primary value to privacy claims, has high organizational distrust, and advocates comprehensive privacy interventions through legal rules and enforcement. A limited-privacy position views privacy claims as usually less worthy than business efficiency and societal-protection interests, is generally trustful of organizations, and opposes most new regulatory interventions as unnecessary and costly. A balanced-privacy position values privacy strongly but seeks tailored legal interventions that address demonstrated abuses, along with voluntary organizational-policy initiatives intended to promote individual privacy choices. The relative size and influence of these positions has varied across the time periods treated. (For discussions of the politics of privacy, see Gandy, this issue; Regan, 1995; Rule, McAdam, Stearns, & Uglow, 1980; Strum, 1998; and Westin, 1991)

Full disclosure leads me to locate myself somewhere between the balanced-privacy and high-privacy positions, depending on the issue. Since 1952, I have been a social scientist studying the impact of technology and social change on privacy through empirical inquiries (Barber, 1987), a privacy champion in publications and legislative/regulatory testimony, and a privacy consultant to government and

business organizations. Therefore, in writing my account of the privacy scene from 1945 to the present, I have tried to make my assumptions as transparent in premises as possible, allowing readers to evaluate my judgments from their own ideological perspectives and interests. Many of the historical and political judgments presented here are made as a participant-observer, not from third-party commentaries or histories.

The Privacy Baseline, 1945–1960

The 15 years after the close of World War II were a period of limited information-technology developments (Westin, 1967; Westin & Baker, 1972). There was high public trust in government, business, and the non-profit sector and, therefore, general public comfort with the information collection and use activities of those organizations. Majorities approved of the allocable standards (e.g. race, gender, sexual orientation) that institutions used for deciding on the rights, benefits, and opportunities of individuals in an increasingly record-keeping and credential-based social system. The mass media generally accepted privacy limits in its coverage of political actors and public life. Law addressed privacy issues in traditional constitutional and common law concepts, accepting business-marketing practices and employer uses of personal information as not violating any personal legal rights.

There were substantial intrusions into personal and associational privacy through government loyalty-security programs, private blacklists and congressional hearings during what is called the Joseph McCarthy era. However, reflecting strong public anti-communist attitudes, neither courts nor legislatures placed limits on these activities before 1960 (Westin, 1967, Part Four; Westin & Baker, 1972).

In short, while there were important civil liberties and civil rights struggles in this era, neither public nor legal discourse was organized around a free-standing right-to-informational privacy theme. Privacy was essentially a third-level social issue—interesting but neither primary nor even secondary in social and political salience.

The First Era of Contemporary Privacy Development, 1961–1979

This period marked the rise of information privacy as an explicit social, political, and legal issue of the high-technology age (Miller, 1971; Westin, 1967). It was a turbulent era that included civil rights struggles, anti-war and other social-protest movements, the sexual revolution, and Watergate. Within this social climate, concerns over privacy developed in a familiar new-social-issues pattern: early alarms, empirical studies, alternative policy formulations, and first-generation legal and organizational actions. My description of the pattern follows.

Advances in physical, psychological, and data surveillance technologies were made and widely embraced by government and private-sector institutions in the early 1960s (Westin, 1967, Part Two). By the mid-1960s, what came to be called central data bank projects, using newly-arrived third-generation computer mainframe systems with remote access, were being developed by local and state governments, major businesses, and the federal government. Most of the popular media in the early 1960s applauded the positive improvements in organizational decision-making and administration these technologies seemingly offered (Westin, 1971).

However, recognizing the potentially dark side of the new technologies, popular commentators sounded privacy alarms (Brenton, 1964; Packard, 1964) that were widely echoed in the mass media. My own book, *Privacy and Freedom* (Westin, 1967), analyzed the nature and functions of privacy, privacy's social roles in democratic society, the new surveillance technologies and their widespread embrace, and the breakdown of the once-vibrant U.S. privacy legal framework. I called for new privacy standards and protective actions (Westin, 1967).

These early alarms led the United States and other democratic nations to initiate government commissions and private-sector empirical studies that investigated the nature, dynamics, and impacts of technology applications and explored ways to define and apply new privacy balances (Bennett, 1992). In the United States, a National Academy of Sciences (NAS) study examined, in depth, computer uses and privacy effects in 55 advanced government and private-sector organizations, across 14 sectors, that collected personal data (Westin & Baker, 1972). The study found that computer adoptions in these 55 organizations that collected personal data had not yet significantly transformed existing privacy relationships, largely because of high data processing and storage costs, software limitations, and organizational guarding of databases as competitive assets. However, the study predicted that lowered costs and software progress would allow organizations in the later 1970s and beyond to automate personal information much more extensively and to potentially transform decision-making activities. Given the dramatic changes in standards for social allocations unfolding in the 1970s—specifically rejection of previously widespread racial, religious, political and gender discrimination patterns embedded in many existing organizational record systems—the NAS study concluded that positive legislation defining privacy rights would be essential, and laid out a recommended privacy code.

In the same vein, an influential study by an Advisory Committee to the U.S. Department of Health, Education and Welfare (U.S. Department of Health, Education, and Welfare, 1973) formulated a Fair Information Practices (FIP) framework. This combined privacy standards with due process, consumer rights, and equality protections; however, it looked to sectoral, not generic, privacy legislation. Fair Information Practices became the dominant U.S. approach to information-privacy protection for the next three decades.

In socio-cultural terms, this era saw fundamental change in public and private allocable criteria, limiting overt discrimination based on race, gender, family-life conformity, sexual activity, and the like. This required revising all business and government record systems that embedded the older criteria, transforming these personal characteristics into private matters (Westin & Baker, 1972).

In the consumer reporting or credit bureau industry, the presence of closed record systems and the application of suspect criteria to 110 million consumers in bureau files, plus the late-1960s move by this industry to automate its records, produced wide public concerns (Garfinkel, 2000; Smith, 2000). This led to enactment of the first federal fair information practices law—the Fair Credit Reporting Act of 1970. This provided front-end notice, consumer access, and correction rights but did not try to set relevance or privacy standards for consumer reporting.

In political terms, the late 1960s and 1970s saw a majority of the American public shift from general trust in institutions to dramatic distrust (Nye, Zelikow, & King, 1997). FBI and CIA excesses, the Watergate episode, and other Nixon Administration intrusions provided the concrete examples of government abuse of power that made enactment of the federal Privacy Act of 1974 politically possible. Other federal laws followed, such as the Family and Educational Rights and Privacy Act (1974) and the Right to Financial Privacy Act (1978). In addition, prompted by warning decisions from the Warren Supreme Court, Congress finally brought wiretapping under court-order and operating-safeguards legislation, in title III of the Omnibus Crime Control and Safe Streets Act (1968). Also, many states adopted fair information practices acts for government files.

The Privacy Protection Study Commission (PPSC) was created by the federal Privacy Act of 1974 to examine whether the fair information practices approach installed for federal government records about individuals should be extended by Congress to state governments and the private sector. The PPSC conducted a landmark study of private-sector information practices, concluding in its report that state laws and private-sector initiatives were the immediate best steps, rather than an omnibus federal law and a federal privacy regulatory agency (Privacy Protection Study Commission, 1977).

In political terms, a consensus emerged that data banks should not be allowed to consolidate citizen information from separate local or national government agency files, even if this might provide a more complete picture of citizen-government relationships. Though not expressed in law, this consensus governed databank applications throughout this and the next period of privacy developments. Another political fact in this period was that privacy did not always track traditional liberal-conservative ideological lines. In fact, liberals and libertarian-oriented conservatives were frequently united on privacy issues.

Of major importance in this era was the rise of advocacy journalism and television-age media competition. To reporters and editors weaned on exposing Watergate and J. Edgar Hoover's secret files, attacking the privacy invasions of

other institutions and warning the public about various big brothers became a regular exercise. At the same time, the media became, in this era, one of the major invaders of privacy of both the famous and anyone else caught up in public events. These intrusions were justified in the name of the public's right to know, but many were clearly driven to burnish journalistic reputations and increase media profits.

Beginning in the late 1960s, this era saw a flowering of creative social science examinations of privacy, covering both information-privacy and personal-autonomy issues (e.g., birth control, abortion, drug use, homosexuality, and suicide). Margulis (1977) and Westin (in preparation) analyze these behavioral and social science contributions (see also Mack, 2001; Westin, 2002).

An in-depth picture of U.S. privacy attitudes and policy preferences in this era was captured in 1978 in *The Dimensions of Privacy*, the first detailed national survey of American public views across the full range of citizen, consumer, and employee privacy domains (Louis Harris & Associates & Westin, 1979). Some highlights of the survey's extensive findings follow.

In their interpersonal and daily lives, Americans reported in 1978 that their privacy was actually in good shape. Ninety-four percent felt they had someone they could share their personal problems with when they needed to; 88% felt they were generally able to be by themselves when they needed to be; 89% did *not* feel that their neighbors knew too much about their personal lives; and 67% did *not* feel there was too little peace and quiet in today's world. Over three quarters (78%) said they had *never* personally been the victim of what they felt was an improper invasion of privacy. However, 64% of the public were concerned about threats to their personal privacy in America, up from 34% in 1970.

In questions dealing with credit reporting, insurance, doctors and hospitals, government, and employment, majorities distinguished pragmatically between what they saw as legitimate organizational risk-assessment inquiries and those they felt were too intrusive. (For a study of drawing these lines in the choice of pre-employment selection procedures, see Stone-Romero, Stone, & Hyatt, this issue.) Majorities of the public in 1978 said they felt Congress should pass privacy legislation in the specific areas of health, insurance, employment, and mailing lists.

Analysis of the 1978 survey included the Westin Distrust Index, created by combining respondents' answers to four questions that asked about their trust in government and voting and their attitudes toward business and technology. The survey found 49% of the public in 1978 had high or medium distrust, 34% had low distrust; and 17% were not distrustful. The survey found that the higher the distrust score, the greater the respondent's privacy concerns, hostility to business and government information practices, support for privacy-protection legislation, and so forth.

Overall, with privacy now elevated to a second-level social policy issue, the 1960s and 1970s were a time of substantial privacy scholarship, new social-impact-of-technology analytic methodologies, and creative first-generation information-age privacy laws.

The Second Era of Privacy Development, 1980–1989

Technologically, this was a period of enhanced computer and telecommunications performance but without fundamental changes in information-society relationships bearing on privacy. Distributed computing was added to central data banks. Workplace video display terminals (VDTs) and the personal computer (PC) arrived. The PC marked the first time that computer developments provided power to individuals, rather than being high-cost monopolies of organizations. However, this did not, as yet, affect the privacy situation because PCs were unconnected to the larger world. There were no major developments in physical or psychological surveillance technologies in this period, and genomic research advances lay ahead.

On the whole, business and government activities involving the collection and uses of personal information did not break new ground. While business and government databank operations became cheaper and more efficient, the public remained hostile to combining information from separate government agencies into central databanks, or to unifying the information resources of separate industry lines. This opposition, as well as ownership and competitive reasons for keeping separate databases, blocked such amalgamations. And, where there were exchanges of file data between federal agencies, for example, to cross-check public assistance and employment records to detect fraud, the federal Computer Matching and Privacy Protection Act of 1988 created procedural protections for such file matches.

Politically, privacy remained a second-tier social policy issue in this period, often in play but not a compelling political cause. Privacy protection legislation was championed primarily by traditional liberal groups—the American Civil Liberties Union (ACLU), labor unions, and consumer organizations such as the National Consumers League—though they were often joined by industry groups or conservatives when the issues involved surveillance activities by *governmental* bodies. Two influential privacy newsletters—Robert Ellis Smith's *Privacy Journal* and Evan Hendrick's *Privacy Times*—provided advocacy-oriented coverage of privacy issues that fed the mainstream media, were read by organizational staffs, and informed academic and legal privacy experts.

While a few questions about privacy issues appeared on major national surveys in this period, only one national survey provided in-depth analysis: *The Road to 1984* (Louis Harris & Associates, 1984). This survey documented an essentially rational ambivalence of the public toward new information technologies—warm

appreciation of the benefits and conveniences but gnawing worries about potential misuses and abuses.

This era saw a significant amount of federal legislation adopted to channel new technology applications or new governmental activities into fair information practices or privacy protection frameworks. These included the Privacy Protection Act of 1980, requiring a reasonable basis for suspicion that a crime has been committed before government agencies can make unannounced searches of press offices; the Cable Communications Policy Act of 1984, requiring cable companies to inform subscribers about information collection practices and providing subscriber access rights; the Electronic Communications Privacy Act of 1986, extending the 1968 wiretap court-order and control procedures to digital voice data and video communications; and the Video Privacy Protection Act of 1988, prohibiting video stores from disclosing their customers' names and addresses and the videos they rent or buy. While not meeting all the wishes of the high-privacy champions, this battery of federal privacy laws demonstrated the salience of privacy as a political issue, the inability of the limited-privacy camp to block tailored privacy legislation, and the application of what I have called the dominant U.S. approach—the position of the balanced-privacy supporters.

As for employment, the equality revolutions of the 1960s and 1970s, new social tolerance for diversity in lifestyles, and the need to hire and retain talented professionals and managers led most business and government employers to withdraw from oversight of personal lives in both hiring and personnel administration (Westin, 1979). However, the proliferation of VDTs at work, especially for data entry and customer service operations, led to extensive VDT-work monitoring by American employers, under broad employer-prerogatives legal rules. Unions and civil liberties groups protested about electronic sweatshops. But majorities of the public and American employment law supported employer use of monitoring practices, if reasonable (Westin, Baker, Lehman, & Schweder, 1985). Codes of fair monitoring practices were developed in the financial and telecommunication industries, and these became widely observed. In 1988, Congress passed the Employee Polygraph Protection Act, prohibiting most private-employer uses of lie detector tests.

While the United States remained committed to a fair-information practices and sector-based regulatory approach, European nations moved, in the early 1970s, into a different mode—national data protection laws covering the entire governmental and private sectors, under independent national data protection agencies (Flaherty, 1979; Schwartz & Reidenberg, 1996). By the late 1980s, many European nations, such as Germany, Sweden, France, and Britain, had enacted and were operating under such data protection laws (Simitis, 1987). While the European model was not adopted in the United States, influential privacy guidelines adopted by the Organization for Economic Cooperation and Development (OECD) in 1980 (OECD, 1980) were praised by the Reagan Administration, recommended for

voluntary business adoption by the National Telecommunication and Information Administration (NTIA), and written into formal employee or consumer privacy policies by almost 200 American companies by the early 1990s. However, there was no legal mechanism to oversee the application of these OECD-modeled codes, no individual lawsuits available to invoke rights under them, and little restrictive impact on business information practices in this period (Gellman, 1996).

In addition to a flood of writings about privacy in law reviews, this era saw a rich development of social science analyses. Many of these writings are discussed in this issue, passim, and are analyzed under each major social science discipline in Westin (in preparation).

Overall, 1980–1989 can be seen now as a period of relative calm before the storm.

The Third Era of Privacy Development, 1990–2002

This is the period when privacy became a first-level social and political issue in the United States, assumed global proportions, and was impacted by 9/11 and its aftermath.

At least five major developments in technology in this period framed the privacy debates. First, and the most far-reaching, was the rise of the Internet in the mid-1990s; by 2001, over 100 million individuals were exchanging personal and business e-mails, searching for information, shopping, and participating in online forums, usually as a daily routine and with high self-disclosure. Second was the arrival of wireless communication devices—the now ubiquitous cell phone (137 million instruments in February 2003)—that made telephone communication instantly mobile and convenient (Cellular Telecommunications and Internet Association [CTIA], 2003). Third, and adding still another domain to the technology-privacy interface, was the Human Genome Project's unlocking of the genetic code, with enormous promise for use in developing new pharmaceutical medications, family planning, and health care. Fourth was the development of data-mining software based on large data warehousing applications, along with further automation of government public record systems. This made it possible for American consumer businesses to move from industrial-age mass marketing to personalized target marketing, producing in-depth consumer profiles by combining databases of personal transaction records about consumers with overlays from public record sources, provided by information supplier companies. Finally, federal law enforcement and national security agencies worried that strong encryption programs could immunize online communications by drug dealers and terrorists from lawful surveillance. This prompted government efforts to block private use of encryption tools and also to develop the FBI's Carnivore program for accessing online communications.

While the technological developments just noted brought many positive features to consumer life and societal protection, they also generated privacy alarms

from both the high-privacy and balanced-privacy camps. There was concern over Web sites using tracking devices such as cookies to identify visitors and document their usage, even if businesses said they were doing this for site improvement or marketing purposes. Wireless communication devices brought the capability of government law enforcers or private litigators to locate individual users by time and place through mobile technology, and also the potentiality of companies sending marketing messages to wireless users based on knowing their location near particular business establishments. The prospect that genetic tests might be required for determining access to health or life insurance or employment, and could impose doubtful standards of likely health progress on millions of persons, made setting privacy rules for genetic information a major battlefield. This was especially acute as computerization promised to finally re-organize American health care into an electronically based system in the 2000–2010 decade. (For a discussion of genetic and medical privacy, see Alpert, this issue.)

The rise of identity theft as a personal-data-based white collar crime in the late 1990s, along with highly publicized stalking cases based on accessing public record files, raised major issues about the security and privacy of personal data in business and government record systems. In consumer marketing, the technology-based business model of the 1990s—we must know you to serve you—came into fundamental collision with the now dominant consumer model—let me decide what you know about me, thanks.

Finally, federal efforts to limit encryption software drew challenges from the technology industry and civil libertarians. A rough accommodation between government needs and privacy rules had been achieved by the time that the 9/11 events changed the situation dramatically.

The social and economic climate in which these technology applications unfolded was one of high overall prosperity, fueled by a vibrant consumer-marketing system, peace and security in the international arena, and an indulgent, me-centered social milieu. While customized marketing helped link business offers to individualized lifestyles and interests, expanded mail marketing and especially telemarketing in the 1990s drew increased consumer annoyance. And, the mass media continued negative coverage of what was portrayed as privacy-intrusive business marketing (Garfinkel, 2000; Larson, 1992).

A major development in this period was the globalization of the privacy issue, driven by rising worldwide communication, trade, travel, and marketing activities. Global use of credit cards and Internet use typified the trend, which produced the collection and use of consumer transaction and communication data by multinational companies. The new European Union (EU) sought, in the early 1990s, to encourage the flow of commerce and information among its 15 member nations and also to set European-style data protection rules and regulatory administration for cross-border data transfers. This resulted in the EU Data Protection Directive (EU Directive 95/46/EC, 1995), which mandated (after 1998) that personal data

on consumers and employees could not be transferred by multi-national firms operating in the EU back to their home nation unless that country had what the EU considered an adequate data protection regime, or qualified for special procedures. Adequacy required a comprehensive law applying EU data protection standards to both the private and public sectors and a national regulatory system providing enforceable legal rights. Faced by the possibility that U.S. firms operating in the EU would not be able to transfer personal data on consumers and employees to U.S. processing sites, policy debates in 1997–2000 included sharp discussions of whether the United States should adopt the EU model, ignore the directive as a non-tariff trade barrier to be fought, or try to find some way of accommodation. (For further discussion of EU-U.S. data-transfer relationships, see Regan, this issue.)

Interest groups generally followed the high-, limited-, and balanced-privacy positions, already noted, but with some new issues and stances. Several liberal-oriented public interest organizations focusing on technology-society relations emerged (e.g., the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the Center for Democracy and Technology). Joining existing civil liberties and consumer-rights groups, a broad coalition of self-described "privacy advocates" collected examples of alleged intrusive business and government data-uses, fed these to sympathetic mass media reporters, and became key players at privacy legislative and regulatory proceedings. In 1993, I founded Privacy and American Business, to provide a privacy-sensitive but business-friendly non-profit center for research and education (http://www.pandab.org).

Business interests, in general, opposed comprehensive privacy regulation, viewing this as an unnecessary interference with business communications and consumer choice and raising serious First Amendment constitutional issues (Cate, 1997). Industry groups cited high compliance costs and likely class-action litigation as reasons to avoid sweeping consumer-privacy laws. However, many consumer businesses watched the survey results and negative media stories and concluded that privacy concerns deserved good responses. In the early 1990s, my judgment was that about 5–10% of consumer-product companies adopted pro-active, voluntary privacy policies reflecting fair information practices (FIP) rules. An additional 30–40%, and even more online, moved to such positions in the mid- to late 1990s, led by new privacy-accepting industry groups such as the Online Privacy Alliance. But the majority of consumer businesses, especially off the Internet, did not embrace FIP standards voluntarily in the mid- to late 1990s, and most mainline business groups opposed privacy bills drafted in Congress and many states. An exception to this pattern was the federal Children's Online Privacy Protection Act, which was enacted with general business support.

Popular culture in this era featured a steady drumbeat of invasion of privacy articles in newspapers and magazines, on radio and television shows, and in lurid feature movies, such as *The Net* (Winkler, Cowan & Winkler, 1995), *Gattaca*

(DeVito & Niccol, 1997), and *Enemy of the State* (Bruckheimer & Scott, 1998). At the same time that the mass media was critically featuring alleged privacy intrusions by business and government, the mass media itself engaged in increasingly privacy-intrusive and sensationalized journalism (Gurstein, 1996). This period saw also the flowering of voyeur television—shows on major networks featuring persons confessing to large viewing audiences the most intimate features of their sexual and personal lives, and TV "reality programs" filming personal intimacies. This trend not only shattered previous boundaries of broadcast reserve but also prior lines of civility in popular culture (Calvert, 2000).

Of importance in this decade was a stream of more than 120 national surveys either wholly or in significant part probing public attitudes toward privacy (see Westin, 2002, for a survey bibliography; also see Gandy, this issue). These surveys varied widely in quality and sponsor imprint and prompted sharp debates not only over the sophistication of or bias in the questions used but also over whether privacy survey results provided a sound basis for formulating public policies on privacy. In the years from 1990 to 1995, my reading of this body of surveys shows virtually all the results, whether sponsored by business, consumer groups, or academics, showing privacy rising steadily as a public worry. The major differences involved measurement of attitudes toward regulation or self-regulation, expression of consumer choice orientations in various contexts, levels of trust or distrust in various industries or Internet operations, and policy implications to be drawn from acknowledged levels of consumer privacy concern. My analysis of survey trends in this period, which follows, will rely on my own surveys with Louis Harris & Associates, Harris Interactive, and the Opinion Research Corporation, between 1990 and 2002.

Reports of individuals managing privacy interests in their daily lives remained in the same positive mode as reported in 1978 (Louis Harris & Associates & Westin, 1990). However, fears about privacy invasions in the social and political world rose to new heights in the 1990s. Respondent concern about threats to personal privacy jumped from 64% in 1978 to 84% in 1995. This reflected a sharp rise in high and medium distrust from 49% in 1978 to 71% in 1995. While 51% felt that government posed the largest potential threat to privacy, 43% instead cited business. Financial and health information were identified as the types of personal information the public considered most sensitive. While majorities were still avid consumers and approved of various kinds of marketing and profiling with notice and choice policies, 80% agreed by 1995 with the statement that consumers "have lost all control over how companies collect and use consumer personal information." In this climate, American consumers began exercising individual privacy assertiveness, with 59% saying they had refused to give information to a business because they felt it was too personal or not really needed.

Turning to privacy in personal lives, an unpublished Harris-Westin survey in 2001 (Harris Interactive & Westin, 2001b) repeated items from an unpublished Harris-Westin survey in 1994 (Louis Harris & Associates & Westin, 1994).

Noting that "privacy means different things to different people," the survey asked respondents to rate the importance to them of several "different aspects of privacy." Four statements were presented expressing the privacy states from Westin's (1967) *Privacy and Freedom*. Intimacy was rated by the American public by far as the most "extremely important" of the four states of privacy, at 81%. Solitude was second at 66%, reserve at 55% and anonymity at 47%.

As for employee privacy, a 1993 survey of private-sector employees found very high satisfaction with the information practices of their employers, in sharp contrast to the consumer-privacy trends (Louis Harris & Associates & Westin, 1993). Only a minority of employees, under 20%, felt that their employers were violating various employee privacy rights presented in the survey.

In 1995, Harris-Westin surveys began to segment the public on consumer privacy issues, producing a division that essentially mirrored the three ideological-interest positions (Louis Harris & Associates & Westin, 1995). What we called *privacy fundamentalists* were 25% of the public who, like high-privacy oriented proponents, rejected consumer-benefit or societal-protection claims for data uses and sought legal-regulatory privacy measures. Akin to the limited-privacy camp, the *privacy unconcerned*, at 20%, were generally ready to supply their personal information to business and government and rejected what was seen as too much privacy fuss. Between these two camps, like the balanced-privacy position, were *privacy pragmatists*, at 55%. They examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organizations proposed to control those, and then decided whether to trust the organization or seek legal oversight. The policy struggle of the 1990s was (and remains today) a battle for the mind and hearts of the privacy pragmatists.

In the second phase, 1996–1999, surveys showed that the spread of Internet use was dramatically increasing overall public concerns about privacy. There was opposition to Web sites tracking visitors' movements and especially capturing information from or about children using the Internet, along with fears about the security of using credit cards to shop online. By 1999 (Louis Harris & Associates & Westin, 1999), public concern about possible misuse of personal information had risen to 94%. However, 60% still felt that personalized marketing based on customer profiles was a good thing for consumers and 65% agreed with the statement that "most businesses handle customer personal information in a proper and confidential way." Moreover, 59% agreed with the statement that "existing laws and organizational practices provide a reasonable level of consumer protection." As of 1999, the Harris-Westin privacy segmentation remained relatively constant, at 25% privacy fundamentalist, 53% privacy pragmatist, and 22% privacy unconcerned (Louis Harris & Associates & Westin, 1999).

Harris-Westin surveys in 2000–2002 (Harris Interactive & Westin, 2001a, 2001b, 2002a, 2002b, 2002c) recorded a dramatic shift in public attitudes. While belief that consumers had lost control over how their personal information was used by businesses remained high and relatively level at 79%, 56% now felt that

most businesses did *not* handle the personal information they collect in a proper and confidential way (up from 34% in 1999). And 62% did *not* believe that existing laws and organizational practices provided a reasonable level for protection of consumer privacy (up from 38% in 1999). With these major shifts in the results of questions used for our privacy segmentation, the privacy unconcerned dropped from 22% in 1999 to 8% in late 2001. Privacy pragmatists remained the majority, at 58%, but privacy fundamentalists rose from 25% to 34%. Similarly, individual privacy assertiveness climbed, with 87% saying they had refused to give their personal information to a business and 83% saying they had asked to have their name and address removed from a company's marketing lists.

Three primary factors drove the 2000–2002 shift in public mood. First, prospects in 1998–1999 of Congress approving the merger of banks, insurers, and investment companies into single financial service entities promised an end to the traditional separation of consumer personal information in three separate industry silos and a consolidation of consumer financial and insurance information in new cross-market-oriented companies. Second, the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 directed the nation's health sector to move by the early 2000s to electronic systems for processing medical treatment, claims, and administrative data. The fact that there were no general federal laws protecting health-information privacy and only a weak patchwork of state health privacy laws generated health-professional and privacy-advocate outcry and high public concern. Third, dozens of surveys showed widespread apprehension by Internet users about the privacy and security of their online information.

The effect of these developments was to weaken the political middle of the privacy-policy debates. For politicians watching polls and media trends, it was clear by 2000 that championing privacy protection was now very good politics. At the state level, hundreds of new consumer privacy laws were enacted each year in 2000 and 2001, with coalitions of Republican and Democratic political leaders uniting to reflect the privacy concerns of suburbanites, women, Internet users, and other desirable local constituencies. State attorneys general formed a privacy task force and began an aggressive campaign of suing businesses for alleged violations of their privacy promises or obtaining consumer personal data improperly.

At the federal level, over industry opposition, Congress moved to limit traditional open-records access to state driver's license files, in the Drivers Privacy Protection Act of 1994 and also wrote a moderate privacy code into the 1999 Financial Modernization Act. When Congress proved unable to write a health privacy code, it turned that task over to the U.S. Department of Health and Human Services (HHS), which issued a Privacy Rule in late 2000, to go into effect in April 2003. By executive order, in 2000, President Clinton directed that genetic information could not be required in federal employment processes.

The 2000 election campaign exemplified the new consensus on privacy. Both Democrat Al Gore and Republican George W. Bush made speeches promising

to protect financial and health privacy and address Internet privacy needs. Many conservative as well as liberal congressional candidates included support for new privacy protections in their platforms. In all these forums, concerns of business about the costs of compliance, disruption of business, and threats to continued e-commerce expansion—expressed as arguments for relying on self-regulation—were essentially rejected; business lobbyists found themselves working to moderate new laws and able to block only the most sweeping measures. While the new Bush Administration's Federal Trade Commission (FTC) majority declined to recommend federal privacy legislation for the Internet (as the Clinton FTC had done), the Bush FTC promised aggressive enforcement of existing authority to hold Web sites to their announced privacy policies. In early 2001, demonstrating the political force of the public's new privacy attitudes, President Bush declined to follow calls from industry (many from major Republican financial contributors) to postpone and reconsider the strong HHS health Privacy Rule, scheduled to start in 2003 (Privacy Rules, 2000). Bush let the Rule proceed, though HHS made some retrenching interpretations in March of 2002 (HIPAA, 2002). (For a discussion of the final status of the Privacy Rule, see Alpert, this issue.) On another front, consumer privacy litigation expanded significantly under state attorneys general, FTC, and private plaintiff initiatives.

Internationally, to allow their multi-national firms to transfer personal data from Europe to the home country, some major non-EU nations, such as Canada and Australia, enacted national privacy laws for the private sector to meet EU requirements. However, the United States and Japan did not do so (as of late 2002). Instead, the Clinton Administration negotiated with the EU an understanding called "Safe Harbor." This would allow U.S. multinational firms that signed on to follow EU Directive–based policies to move their employee or customer data from EU nations to the United States for processing, under enforcement power from the Federal Trade Commission (FTC). However, as of mid-2002, only about 200 U.S. companies, mostly smaller firms, had signed on to Safe Harbor, and they signed on mostly for transferring personnel data. Whether some of the 15 national data protection agencies in the EU would now move against non-signing U.S. firms and prohibit their transferring personal data from their country to the United States remained unclear, as did how the Bush Administration would act if such steps were taken. In late 2002, the EU opened a reconsideration of the EU Directive's administration, including possible measures to make transborder data transfer rules less stringent and bureaucratic. (For a full treatment of this issue, see Regan, this issue).

In terms of political ideology, an even broader coalition emerged to promote consumer and citizen privacy. If we use a five point scale—left, liberal, centrist or moderate, conservative, and libertarian—the activist left was not engaged in these privacy issues, having their activities focused elsewhere. Liberal, conservative, and libertarian interest groups and leaders united to champion the privacy

cause. However, when it comes to remedies, liberals and many conservatives have embraced government regulation to protect consumer privacy while libertarians generally endorsed market corrections.

And Then Came 9/11

The terrorist attacks of September 11, 2001, dramatically changed the privacy landscape. The magnitude and shock of the terrorist attacks, the likely continuation of terrorist actions within the U.S. "homeland," and the dangerous new types of weapons and techniques involved have promoted national security interests into an urgency unmatched in American experience. Very few observers see the current federal response as an unjustified exercise in the Joseph McCarthy pattern.

We can again draw on survey research to lay out judgments about 9/11 impacts. Because the federal government is responsible for defending citizens from terrorist attacks, and the Bush Administration was seen as handling immediate responses well, public trust in government—President, military, Congress, law enforcement, etc.—soared initially, and with it support for increased investigative powers. A survey done shortly after 9/11 (Harris Interactive & Westin, 2001a) recorded very high public approval of new governmental investigative powers. For example, 93% approved expanded undercover activities in suspected groups, 86% approved facial-recognition technology to scan for terrorists at public events and places, 81% approved closer monitoring of financial transactions, and 68% approved adoption of a national citizen identification system. At the lowest approval level but still a majority, 54% approved of expanded government monitoring of cell phones and e-mails. Overall, a very high 87% believed that law enforcement will use its new powers in a proper way. In the same survey, the public expressed strong concerns about the way these powers might actually be used by U.S. law enforcement. The public worried that judges will not look closely enough at the justifications for surveillance (79%), Congress will not include adequate safeguards in its authorizations (78%), communications of innocent people will be checked (72%), and new surveillance powers will be used to investigate crimes other than terrorism (67%).

By September, 2002, a repeat Harris survey of anti-terrorist measures found that support for some stronger surveillance and law enforcement measures continues while support for others declines (Harris Interactive & Westin, 2002c). Specifically, 60% continue to favor a national ID system and 58% support extended camera surveillance on streets and in public places. However, support for law enforcement monitoring of Internet forums fell to 42% in September 2002, and support for government monitoring of cell phones and e-mail fell to 32%.

The public's future attitudes will likely turn on two central factors: (a) whether there are more successful terrorist attacks, thereby deepening a sense of crisis and support for extensive surveillance, and (b) published accounts of how the

government is using its new powers, whether carefully and, consequently, deserving continued public support or with abuses that would alarm the public and spur calls for more civil-liberties-oriented controls. These factors will unfold in a return-to-normal political environment, debating issues such as why government failed to connect the dots of available intelligence to predict and forestall terrorist attacks between 1993 and 2001 and how to reorganize the federal intelligence and homeland security apparatus and processes.

While 9/11 altered citizen-government privacy balances into the foreseeable future, consumer privacy issues have remained essentially the same; increased trust in government has not been matched by any increased trust in business. A survey of Internet users in early 2002 found that 87% were still concerned about privacy threats when they went to shop or seek information online (Harris Interactive & Westin, 2002a). When asked how the 9/11 events affected their views of *consumer* privacy issues, 74% said they remained as concerned as before and 26% said they were even more concerned now. Only 1% said they were less concerned.

As for employee privacy post 9/11, a 2002 Harris-Westin survey of government, business, and non-profit employees (Harris Interactive & Westin, 2002b) found continued high approval of employer information practices across all three sectors, paralleling the Louis Harris & Associates and Westin (1993) results described earlier in this article. Seventy-six percent of employees in 2002 rate their employers' "privacy rules and practices" as pretty good to excellent. They do not believe their current employer has asked them for personal information they thought was not appropriate (88%). However, 30% of employees expressed concern about some of their employers' handling of personal employee data. These were the same respondents who voiced perceptions of overall unfair personnel practices, suggesting that employee privacy concerns reflect perceptions of (and probably the reality of) badly-managed workplaces.

Some Predictions

While I foresee little privacy legislation in the employee privacy domain in the next few years, I see major new legislation, enforcement, and litigation unfolding in the consumer privacy arena in 2003–2005. This will lead businesses, both offline and online, to install comprehensive privacy-management systems and to appoint privacy officers to administer compliance. Consumer marketing will move inexorably to a permission-based system, in which consumers exercise their choices as to how they are marketed to, in a mixture of "opt-in" and "opt-out" procedures based on the sensitivity of the data (e.g., Culnan & Bies, this issue). Easy-to-use individual privacy management software will be developed to allow consumer choices to be understood and carried out in both the offline and online venues. Public record laws will be re-written to allow greater access through Internet dissemination while also protecting privacy interests (e.g. suppressing the

home addresses of judges and police in real estate records). Telemarketing will be sharply curtailed as an intrusion the great majority of Americans are no longer willing to tolerate (through legislated "do not call" lists set up by state governments, and possibly a national do not call system); however, control of online spam (unsolicited e-mails) will continue to prove difficult, owing to the borderless and manipulatable features of the World Wide Web.

Building privacy controls into emerging technologies, such as intelligent vehicle highway systems, genetic testing, and satellite-based mobile voice and data systems, will require strong effort, as will seeing that enhanced identification tools such as biometrics are held to high accuracy requirements and used in a proper way, along with developing online privacy-enhancing technologies that are both effective and user-friendly. Privacy rules and enforcement actions among most democratic nations will be broadly harmonized and consumers will navigate Web sites in these jurisdictions with general confidence. However, commercial Internet activities mounted from anti-democratic nations and nations-of-convenience will divide the world into privacy-respecting and privacy-ignoring locations, making *caveat surfer* and use of blocking technologies the online privacy commandment.

Managing personal states of privacy, from healthy solitude and intimacy to positive self-disclosure, will remain as challenging for the individual American as ever. The astonishingly high self-revelations in which many on the Internet engage, and the continuing waves of TV and Internet voyeurism noted earlier, promise to weaken even further the boundaries of privacy and reserve in the United States, especially among the young generation weaned on a "let it all hang out" philosophy.

Citizen privacy issues will be the most troublesome, and achievement of acceptable democratic balances the most problematic. Given terrorist threats, I see increased use of law-enforcement video camera systems in public places as likely, along with adoption of biometric identifier systems by many government and private organizations. Some form of national ID system seems to me inevitable within the next few years.

Limiting surveillance and monitoring powers given to law enforcement is always challenging (see Marx, this issue) and this will be even more so in a terrorist-threatened world. As we learn why pre-9/11 intelligence failed, as additional terrorist attacks occur and our planning to avert them is studied, and as anticipation of new terrorist threats takes place, we can hope that the institutional mechanisms our society uses to control investigative excesses will be applied. These include active judicial oversight of surveillance systems, civil liberties and privacy group studies and advocacy, media exposures of surveillance-system violations and investigative wrong-doing, continuing executive-agency reviews of working procedures, and legislative investigations resulting in installation of effective legislative safeguards. None of this will be easy. A loss of overall citizen privacy in America's post-9/11, compared to the pre-9/11, eras, analyzed in this article, will surely be the judgment of 22nd century historians. Whether the new

privacy balances will be seen as a necessary and justified shrinkage or a disastrous and authority-abused decline remains to be seen.

Conclusion

As this issue of the *Journal of Social Issues* amply documents, privacy issues now permeate many facets of our individual and family lives, our social and cultural milieu, our state and national politics, and key relationships of us all with employers, businesses, and government. We have come to realize that how well democracies balance the competing demands of privacy, disclosure, and surveillance will exert a major influence on the quality of civic life in the 21st century, and that shaping this balance will now have to be done in the context of continuing terrorist threats and actions.

In short, privacy is a quality of life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all.

References

Barber, B. (1987). A. F. Westin: The protection of privacy in the public and private sectors. In *Effective Social Science* (pp. 125–151). New York: Russell Sage.

Bennett, C. J. (1992). *Regulating privacy*. Ithaca: Cornell University Press.

Bennett, C. J. (in preparation). Privacy in the political system: Perspectives from political science and economics. In A. Westin (Ed.), Privacy and Freedom *updated: Social science perspectives on privacy*.

Brenton, M. (1964). *The privacy invaders*. New York: Coward McCann.

Bruckheimer, J. (Producer), & Scott, T. (Director). (1998). *Enemy of the state* [Motion picture]. United States: Buena Vista.

Cable Communications Policy Act of 1984, 47 U.S.C.A. § 551.

Calvert, C. (2000). *Voyeur nation*. Boulder, CO: Westview Press

Cate, F. H. (1997). *Privacy in the information age*. Washington, DC: Brookings Institution.

Cellular Telecommunications and Internet Association [CTIA]. (2003). Retrieved February 28, 2003, from http://www.ctia.org

Children's Online Privacy Protection Act of 1998, 15 U.S.C.A. § 6501 *et seq*.

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C.A. § 552a.

DeVito, D. (Producer), & Niccol, A. (Director). (1997). *Gattaca* [Motion picture]. United States: Columbia.

Drivers Privacy Protection Act of 1994, 18 U.S.C.A. § 2721 *et seq*.

Electronic Communications Privacy Act of 1986, 18 U.S.C.A. § 2510 *et seq*.

Employee Polygraph Protection Act of 1988, 29 U.S.C.A. § 2001 *et seq*.

EU Directive 95/46/EC (1995), *EU Official Journal L 281*, 23/11/1995 pp. 0031–0051. Retrieved from http://www.europa.eu.int/comm/internal/en/dataprot/law/index.htm

Fair Credit Reporting Act of 1970, 15 U.S.C.A. § 1681 *et seq*.

Family and Educational Rights and Privacy Act of 1974, 20 U.S.C.A. § 1232g.

Financial Modernization Act of 1999, 15 U.S.C.A. § 6801 *et seq.*

Flaherty, D. (1979). *Privacy and government data banks: An international perspective*. London: Mansell Publishing.

Garfinkel, S. (2000). *Database nation*. Sebastopol, CA.: O'Reilly.

Geller, G. (in preparation). Privacy in groups and community: Perspectives from anthropology and sociology. In A. Westin (Ed.), Privacy and Freedom *updated: Social science perspectives on privacy*.

Gellman, R. M. (1996). Can privacy be regulated effectively on a national level: Thoughts on the possible need for international privacy rules. *Villanova Law Review*, *41*(129), 155–156.
Gurstein, R. (1996). *The repeal of reticence*. New York: Hill and Wang.
Harris Interactive & Westin, A. (2001a). *The Harris poll: #49*. New York: Harris Interactive.
Harris Interactive & Westin, A. (2001b). *The Harris poll*. Unpublished manuscript. New York: Harris Interactive.
Harris Interactive & Westin, A. (2002a). *Privacy on and off the Internet: What consumers want*. Hackensack, NJ: Privacy & American Business.
Harris Interactive & Westin, A. (2002b). *Privacy and security: The mind and mood of U.S. employees and managers*. Hackensack, NJ: Privacy & American Business.
Harris Interactive & Westin, A. (2002c). *The Harris Poll #46*. New York: Harris Interactive.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. LL. No. 104-191.
Health Insurance Portability and Accountability Act (HIPAA), 67 Fed Reg. 14775–14815 (2002, March 27). (HHS proposed changes).
Larson, E. (1992). *The naked consumer*. New York: Henry Holt.
Louis Harris & Associates. (1984). *The road to 1984*. New York: Louis Harris & Associates.
Louis Harris & Associates & Westin, A. (1979). *The dimensions of privacy*. New York: Louis Harris & Associates.
Louis Harris & Associates & Westin, A. (1990). *The Equifax report on consumers in the information age*. Atlanta, GA: Equifax, Inc.
Louis Harris & Associates & Westin, A. (1993). *Workplace health and privacy issues: A survey of private sector employees and leaders*. New York: Louis Harris & Associates.
Louis Harris & Associates & Westin, A. F. (1994). [Unpublished survey report]. Unpublished raw data.
Louis Harris & Associates & Westin, A. F. (1995). *Equifax-Harris mid-decade consumer privacy survey*. Atlanta, GA: Equifax, Inc.
Louis Harris & Associates & Westin, A. (1999). *The IBM-Harris multi-national consumer privacy report*. New York: IBM.
Mack, A. (Ed.). (2001). Privacy. *Social Research, 68*(1).
Margulis, S. T. (Ed.). (1977). Privacy as a behavioral phenomenon. *Journal of Social Issues, 33*(3).
Miller, A. R. (1971). *The assault on privacy*. Ann Arbor, MI: University of Michigan Press.
Nye, J. S., Zelikow, P. D., & King, D. C. (1997). *Why people don't trust government*. Cambridge, MA: Harvard University Press.
Organization for Economic Cooperation and Development (OECD). *OECD guidelines on the protection of privacy and transborder flows of personal data (1980)*. Paris: OECD Publications Service.
Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.A. § 2510 *et seq*.
Packard, V. (1964). *The naked society*. New York: David McCay.
Pennock, J. R., & Chapman, J. W. (Eds.). (1971). *Privacy*. New York: Atherton Press.
Privacy Act of 1974, 5 U.S.C.A. § 552 *et seq*.
Privacy Protection Act of 1980, 42 U.S. C. A. § 2000aa.
Privacy Protection Study Commission. (1977). *Personal privacy in an information society*. Washington, DC: U.S. Government Printing Office.
Privacy Rules, 45 C.F.R., § 160 (2000).
Regan, P. M. (1995). *Legislating privacy*. Chapel Hill, NC: University of North Carolina Press.
Regenold, W. (in preparation). Privacy and the self: Perspectives from psychology and psychiatry. In A. F. Westin (Ed.), Privacy and Freedom *updated: Social science perspectives on privacy*.
Right to Financial Privacy Act of 1978, 12 U.S.C.A. § 3401.
Rule, J. B. (1973). *Private lives and public surveillance*. London: Allen Lane.
Rule, J. B., McAdam, D., Stearns, L., & Uglow, D. (1980). *The politics of privacy*. New York: New American Library.
Schwartz, P., & Reidenberg, J. R. (1996). *Data privacy law: A study of United States data protection*. Charlottesville, VA: Michie.
Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review, 13*(March), 707–746.
Smith, R. E. (2000). *Ben Franklin's Web site*. Providence: Privacy Journal.
Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087–1156.

Strum, P. (1998). *Privacy: The debate in the United States Since 1945*. Fort Worth, TX: Harcourt Brace College Publishers.
U.S. Department of Health, Education, and Welfare (1973). *Records, computers and the rights of citizens*. Washington, DC: Author.
Video Privacy Protection Act of 1988, 18 U.S.C.A. § 2710.
Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.
Westin, A. F. (Ed.). (1971). *Information technology in a democracy*. Cambridge, MA: Harvard University Press.
Westin, A. F. (1979). *Computers, personnel administration, and citizen rights* (NBS Special Publication No. 500-50). Washington, DC: National Bureau of Standards, U.S. Department of Commerce.
Westin, A. F. (1991). Privacy and genetic information: A socio-political analysis. In American Association for the Advancement of Science–American Bar Association, M. Frankel, & A. Teich (Eds.), *The genetic frontier: Ethics, low, and policy*. (pp. 53–57). Washington, DC: American Association for the Advancement of Science.
Westin, A. F. (Ed.). (2002). *A classified bibliography of U.S. privacy surveys*. Hackensack, NJ: Center for Social and Legal Research.
Westin, A. F. (Ed.). (in preparation). Privacy and Freedom *updated: Social science perspectives on privacy*.
Westin, A. F., & Baker, M. A. (1972). *Data banks in a free society*. New York: Quadrangle Books.
Westin, A. F., Baker, M. A., Lehman, S., & Schweder, H. (1985). *The changing workplace: A guide to the people, organizational, and regulatory aspects of office technology*. Westchester, NY: Knowledge Industries.
Wheeler, S. (Ed.). (1969). *On record: Files and dossiers in American life*. New York: Russell Sage Foundation.
Winkler, I., & Cowan, R. (Producers), & Winkler, I. (Director). (1995). *The Net*. [Motion picture]. United States: Columbia.

ALAN F. WESTIN, LLB and Ph.D. (political science), is Professor of Public Law and Government Emeritus at Columbia University, where he taught for 37 years, after faculty appointments at Harvard, Yale Law School, and Cornell. He is now President of the Center for Social and Legal Research and head of Privacy and American Business, a non-profit think tank. He wrote his first article on privacy in the Columbia Law Review in 1952, his book *Privacy and Freedom* in 1967, and the National Academy of Sciences study *Data Banks in a Free Society* (with Michael Baker) in 1972. Over the past 50 years, he has served on federal and state privacy commissions, been academic advisor to over 50 national privacy surveys, a consultant on privacy to over 150 government agencies, companies, industry associations, and non-profit organizations, and a keynote speaker at scholarly meetings and privacy conferences around the world.