Robbin, A. (2001). The loss of personal privacy and its consequences for social research. *Journal of Government Information*, *28*(5), 493-527.


Pergamon

Journal of Government Information
28 (2001) 493–527

Journal of Government Information

# The loss of personal privacy and its consequences for social research

Alice Robbin*

*School of Library and Information Science, Indiana University at Bloomington, Bloomington, IN 47405-3907, USA*

Received 5 August 2000; received in revised form 18 November 2000; accepted 3 January 2001

**Abstract**

This article chronicles more than 30 years of public opinion, politics, and law and policy on privacy and confidentiality that have had far-reaching consequences for access by the social research community to administrative and statistical records produced by government. A hostile political environment, public controversy over the decennial census long form, media coverage, and public fears about the vast accumulations of personal information by the private sector were catalysts for a recent proposal by the U.S. Bureau of the Census that would have significantly altered the contents of the 2000 census Public Use Microdata Sample (PUMS). These events show clearly that science does not operate independently from the political sphere but may be transformed by a political world where powerful interests lead government agencies to assume responsibility for privacy protection that can result in reducing access to statistical data. 

*Keywords:* Personal privacy; Confidentiality; Information privacy; Data access; Data sharing; Decennial census; PUMS, Public use microdata sample

## 1. Introduction

More than 30 years of public opinion polls record significant concerns about the quantity and use of personal information collected by the US government and private sector and

* Tel.: +1-812-855-5389; fax: +1-812-855-6166.
*E-mail address*: arobbin@indiana.edu (A. Robbin).

1352-0237/01/$ – see front matter 
PII: S1352-0237(02)00343-X

computer technology whose uses are perceived to diminish personal privacy. During the 1970s, public anxiety was a catalyst for legislative hearings, the enactment of federal and state statutes, and implementation of administrative policies, regulations, and guidelines to safeguard privacy and create enforceable expectations of confidentiality for personal information that was collected by government, financial institutions, and the social research community[1]. Access to government records became restricted. Research on statistical methods to limit disclosure risk made it possible, however, to distribute public use files and summary data tabulations that both protected the confidentiality of respondent information and ensured access to data as a necessary component of scientific discovery and for informed public policy decisions.

The highly charged discourse about public policy and private lives escalated throughout the 1990s, as the government and the private sector collected more personal information and as computer technology moved from the workplace to the home and people connected to the Internet. The mass media trumpeted failures of data security and e-commerce firms' sale of personal information. Public concerns resonated with legislators and government administrators, and they responded with hundreds of bills to protect medical records and financial information, limit the exchange or sale of personal information, and protect the privacy of e-mail communication and a host of other privacy-related issues. Competing interests mobilized as privacy advocates lobbied for greater safeguards and government intervention, while business interest groups opposed government regulation. Just as earlier debates about government intrusion into personal lives had activated the public during the 1970s and changed social scientists' relationship with government, the debates about Internet data security and personal information as big business heightened the sensitivity of government agencies charged with funding research and the social science community that depended on government data.

This article chronicles how public opinion, politics, and law and policy relating to privacy and confidentiality have impacted the social research community's access to government administrative and statistical records. A U.S. Census Bureau proposal for releasing the 2000 Public Use Microdata Sample (PUMS) illustrates how science is not an activity that operates independently from the political sphere. The first part of the article summarizes more than 30 years of public opinion on personal privacy and its relationship to computer technology. The second part discusses how federal and state statutes designed to safeguard personal information collected by government agencies transformed social science's relationship with government since the 1970s. Part 3 is a case study of the public controversy over the decennial census long form. It shows how a hostile political environment, media coverage, and public fears about vast accumulations of personal information led to a U.S. Census Bureau proposal that would significantly alter the contents of the 2000 census PUMS. Part 4 places the Bureau's proposal in the context of congressional inaction, modified institutional relationships, and powerful interests that led government agencies to assume responsibility for privacy protection. The article concludes that it is likely that government agencies will decrease access to statistical data in a response to a political environment perceived to threaten the viability of basic government functions.

## 2. Public opinion surveys on personal privacy, assurances of confidentiality, and the role of computer technology, 1968–2000

Although the word "privacy" does not appear in the US Constitution, public opinion surveys show that most Americans believe that personal privacy is "one of the key things in making this country work, in making this country what it is today," and that privacy is a "right" equal to "life, liberty, and the pursuit of happiness".[2] More than 30 years of public opinion polling shows that privacy is deeply rooted in the American psyche. These surveys record a significant increase in concerns about intrusions into personal life, the quantity and use of personal information collected by government and the private sector, and computer technology uses perceived to threaten personal privacy.[3] The next five sections trace the escalating concerns about privacy since the late 1960s as reflected in public opinion polls conducted by major polling agencies, violations of personal privacy that respondents have experienced, the role that computer technology has played to increase concerns about adequate privacy protection, confidence in assurances of privacy made by business, and confidence in government data collection and record-keeping.

### *2.1. Escalating concerns about personal privacy*

The Louis Harris and Associates polling firm first recorded Americans' general concerns about privacy in March 1968 (Harris Poll #1815). Respondents were asked, "Do you ever tend to feel that sometimes your sense of privacy is being invaded or not—that people are trying to find out things about you that are not any of their business?" Sixty-two percent of the respondents stated that they did not believe that their privacy was being invaded. By the mid-1970s, however, the Watergate Affair and the Nixon Administration's highly publicized wiretapping and surveillance activities radically altered Americans' assessment of the importance of personal privacy. Between March 1974 and April 1978, Americans became very concerned about privacy in their personal life, with between 90% and 97% in March 1974 (Harris Poll #7481) and June 1976 (Harris Poll #7684), respectively, rating privacy as "very important" in their personal life. However, by April 1978 (Harris Poll #7804), the percentage of respondents who ranked privacy as "very important" declined to 79%.[4]

Louis Harris and Associates modified their question wording during the late 1970s to ask respondents about their "level of concern" about "threats of personal privacy in America today." Table 1 shows substantial increases between November 1978 and June 1998 in the number of respondents who said they were "very concerned," from 31% to 52%, with a large jump registered between 1978 and 1983 (31–43%).[5] Overall, the number of people who registered "very concerned" and "somewhat concerned" about personal privacy grew from 63% in 1968 to nearly 90% in 1998. The 20 years of polling data also show a corresponding significant decline in the "not very concerned" and "not concerned at all," from 36% to 8%.

A June 1992 Harris survey found that 66% agreed with the statement that "Personal privacy was not adequately safeguarded" (Harris Poll #924010). Six years later, in June and July 1998, surveys found that about 60% of the respondents were not convinced that

Table 1
Importance of personal privacy, November 1978–June 1998

| How concerned are you about threats to your personal privacy in America today? | Very concerned (%) | Somewhat concerned (%) | Only a little (not very) concerned (%) | Not concerned at all (%) |
|---|---|---|---|---|
| Nov 1978 (Harris #S2826; $N=1511$) | 31.0 | 32.5 | 17.2 | 18.7 |
| Sep 1983 (Harris #832033; $N=1256$)[a] | 47.3 | 29.91 | 15.1 | 7.5 |
| Jan 1990 (Harris #892049; $N=2254$) | 43.7 | 35.3 | 14.6 | 5.9 |
| Jun 1991 (Harris #912046; $N=1255$) | 48.4 | 31.0 | 12.0 | 7.2 |
| Jun 1992 (Harris #924010; $N=1254$) | 47.0 | 30.7 | 12.9 | 7.7 |
| Mar 1992 (Harris #92300; $N=1000$) | 41.1 | 37.9 | 16.0 | 5.0 |
| May 1993 (Harris #931103; $N=1252$) | 56.7 | 28.1 | 10.0 | 4.8 |
| Jul 1993 (Harris #931104; $N=1253$) | 50.0 | 31.3 | 11.5 | 6.0 |
| Jul 1993 (Harris #934009; $N=1000$) | 49.3 | 30.3 | 11.5 | 6.1 |
| Jun 1994 (Harris #943007; $N=1000$) | 48.9 | 32.8 | 12.1 | 5.3 |
| Aug 1994 (Harris #943014; $N=1005$) | 50.8 | 32.6 | 10.4 | 5.3 |
| Jun 1995 (Harris #953012; $N=1006$) | 46.7 | 34.8 | 11.5 | 5.8 |
| Jun 1998 (Harris #738366; $N=1512$) | 52.2 | 34.9 | 9.7 | 3.1 |

Source: Louis Harris' surveys of national probability samples of adults 18 or 21 years or older, available at http://www.irss.unc.edu (June 9, 2000).

[a] The question was slightly modified by the addition of an introductory sentence: Question: 9a "Now, let me ask you about technology and privacy."

their "rights to privacy as a consumer were adequately protected by law or business practice" and more than 44% of respondents believed that consumer privacy protection would get worse or that the situation would remain unchanged (39%) (Harris Polls #738366 and #638114).

### *2.2. Threats to and actual invasions of personal privacy*

During the 1960s and 1970s, Louis Harris and Associates followed this question about "concern about privacy" with a series of questions about particular threats to personal privacy, actual experience, and the source of the threat. Variations on these questions were later asked in the 1980s, 1990s, and early 2000. Early surveys conducted between 1968 and 1976 identified threats coming from family members, neighbors, employees, business, survey polling agencies, telephone company, government, and the computer (Harris Polls #1815, #7481, and #7680). Over this 8-year period, surveys found an increase in the amount of information about personal finances, the number of overheard personal conversations, and close supervision of employees. A series of surveys conducted between March 1974 and 1977, in June 1995, and again in December 1999 found high levels of concern about hospitals and insurance companies' use of medical records and credit bureaus, credit card companies, banks, and government agencies' collection of financial information (Harris Polls #7481, #7483, #7690, #953012, and #11581). A November 1999 Harris survey found an increase in the number of respondents who said that inaccurate information had prevented them from obtaining employment, insurance, and credit (Harris Poll #11490).

Over the past three decades, between 20% and 25% of the respondents have experienced some form of privacy invasion, most likely at the hands of a credit bureau, a government agency, or an individual. This percentage remained unchanged during the late 1990s, increased slightly in early 2000 to 27%, but declined to 15% in late 2000 (Harris Polls #818399, #12059, and #12963). Of those who reported an invasion of privacy in April 1997, more than 13% named government, 43% accused a business, 29.4% named an individual, and 12.5% mentioned ''some other source'' as responsible (Harris Poll #638114). Five percent of the respondents in the April 1997 survey who were computer users indicated that ''their privacy had been invaded when using the Internet'' and nearly 8% of them named their online service provider as responsible. A year later, in June 1998, 40% of the sample identified themselves as victims of an ''improper invasion of privacy by a business'' (Harris Poll #738366).

### *2.3. Personal privacy, computer technology, and the Internet*

Given the recognition of the utility of computers as well as great concern about their potential to diminish personal privacy, it is important to contextualize the trepidation about computer technology. The Louis Harris and Associates polling agency asked a series of questions between 1974 and 1977 that clearly showed Americans believing that the computer provided significant benefits for health, education, safety, and law enforcement (between 84% and 92%) (Harris Polls #7483, #7687, and #7690). From the mid-1970s to 1990, surveys showed that the majority of Americans supported, often by large margins, intrusions into privacy for national security matters, drug testing of employees in critical occupations, corruption, listening in on telephone conversations to monitor worker productivity and quality, and identifying drug smugglers and people with AIDS (Harris Polls #7483, #9119, #874014, #874016, and #892049).[6] A recent survey conducted in 2000 found that more than 90% of the respondents approved of the sharing of corporate-held personal information with law enforcement agencies that ''pertained to fraud, conviction records, and other misconduct'' (McGuire, 2000a). More generally, public opinion surveys have consistently recorded high levels of enthusiasm for computers, with 71% of the public indicating that the new communication technologies have improved the quality of life, according to a recent Pew Research Center (1999) survey.

Nonetheless, there has been a significant increase in anxiety associated with the computer, even as the majority of Americans have become users of the technology (U.S. National Technical Information Administration, 2000). Nonusers are, however, consistently more anxious than users about computer-related risks to personal privacy. Table 2 records public concern about the computer as a threat to privacy between 1968 and 1992.

Perceptions of computer-based privacy violations rose between March 1968 and January 1976 from 18% to about 54%. From the early 1970s to the early 1990s, Harris found that between 38% and 69% of the respondents agreed that computers posed a threat to personal privacy (Louis Harris and Associates, 1984; Louis Harris and Associates & Westin, 1979). In 1983, respondents agreed by large majorities that ''information in computers [is] not adequately safeguarded'' (60%), a ''master file on [yourself]'' constituted a violation of

Table 2
Threats to personal privacy by the computer, 1968–1992

| | Mar 1968 (Harris #1815; $N=1130$) | | Mar 1974 (Harris #7483; $N=1450$) | | Jan 1976 (Harris #7680; $N=1521$)[a] | | Sep 1983 (Harris #832033; $N=1256$)[a] | | Mar 1985 (Harris #861204; $N=1264$)[b] | | Jun 1992 (Harris #924010; $N=1252$)[c] | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Yes (%) | No (%) | Yes (%) | No (%) | Yes (%) | No (%) | Yes (%) | No (%) | Yes (%) | No (%) | Yes (%) | No (%) |
| Do you ever feel your privacy is being violated by computers, which collect and store a lot of information about you[d]? | 18.5 | 72.0 | 34.0 | 57.8 | 39.7 | 53.9 | | | | | | |
| Do you feel that the present uses of computers are an actual threat to personal privacy in this country or not? | | | 38.0 | 41.4 | 37.0 | 50.9 | 54.5 | 31.2 | 70.0 | 26.6 | 68.6 | 28.8 |

Source: Louis Harris' surveys of national probability samples of adults 18 or 21 years or older, available at http://www.irss.unc.edu (June 9, 2000).

[a] Responses: "An actual threat to personal privacy" (Yes), "Not an actual threat to personal privacy" (No), and Not sure (not included in table).

[b] The question reads: "The following statements are concerned with the development of information-processing systems such as computers and word processors. Tell me if you mostly agree or mostly disagree with each of these statements. Item: It will be increasingly possible to use computer data banks to infringe upon personal privacy:" Responses: Mostly agree/Mostly disagree/No opinion (Vol.)/Not sure. "Mostly agree" is "Yes" and "Mostly disagree" is "No."

[c] Wording of question was changed to "Agree very strongly/Agree somewhat strongly/Disagree somewhat strongly/Disagree very strongly/Not sure." "Yes" represents collapsing of "Agree very strongly" and "Agree somewhat strongly" and "No" represents "Disagree somewhat strongly" and "Disagree very strongly."

[d] Wording of introduction slightly altered in March 1974 and January 1976 questions: "Have you ever felt that (read first item on list) infringed on your right to privacy or not?"

privacy (79%), and "the use of computers had to be sharply restricted in the future in order to preserve privacy" (65%) (Harris Poll #8333). By 1985, 70% of Americans agreed with the statement that, "It will be increasingly possible to use computer databanks to infringe upon personal privacy" (Harris Poll #851204). In 1998, a Harris poll found in a national survey that 88% of respondents who were computer users ($n = 459$) were "very concerned" or "somewhat concerned" that the "content of what [was] communicated by e-mail or electronic mail through the Internet would be read by some other person or organization without [their] knowledge or consent" (Harris Poll #818399).

Two years later, a University of California at Los Angeles, Center for Communication Policy (2000) survey of Internet and non-Internet users found additional evidence of public perceptions of the Internet and its relationship to personal privacy. The Center's report noted that, "Privacy has emerged as the subject that raises the greatest concern about the Internet among both users and nonusers" (p. 32). Nearly two-thirds of the Internet users and more than three-quarters of the nonusers agreed with the statement that, "People who go online put their privacy at risk" (p. 32).

### *2.4. Lack of confidence in business*

Business practices regarding personal data appear primarily responsible for people's privacy concerns. Opinion surveys show that consumers do not trust businesses' assurances of privacy. Although consumers say that Web site privacy policies matter, polls show that they have little confidence in companies that provide guarantees of privacy of personal information. For example, a March 2000 survey found that only 10% of the sample maintained that they trusted business "completely," whereas 66% said they trusted business "somewhat" and 24% "not at all" (Harris Poll #12069). However, more than 75% say they would be more likely to use the Internet if the privacy of personal information and communications would be protected (Harris Polls #738226 and #818399).

A 1998 survey of *FamilyPC* magazine subscribers, conducted by researchers at AT&T Laboratories, supports findings from the Harris surveys of the general public, with more detailed information about the concerns of "heavy" Internet users (Crano, Reagle, & Ackerman, 2000). Respondents were "generally comfortable providing preference information to Web companies" but were "often very uncomfortable providing credit card, social security, and telephone numbers" and much less sensitive about providing e-mail addresses. While the "most important factor" in releasing personal information was whether that information would be "shared with other companies and organizations," the willingness to provide personal information depended heavily on how it would be used. Respondents wanted legal protection for using the "information for any purpose other than processing the request," an enforceable company privacy policy, and a seal of approval for the Web company "from a well-known organization such as the Better Business Bureau."

Nonetheless, there is ambivalence about whether business should monitor itself or be regulated by government in order to assure the protection of personal information. A Harris survey conducted in February 1998 asked respondents their opinion on "ways that the government could approach Internet privacy issues. . .at this stage of Internet development"

(Harris Poll #818399). Slightly more than 50% of the respondents said that government should pass laws "now for how personal information can be collected and used on the Internet." Two years later, in March 2000, the percentage of respondents who believed that government "should pass laws now" increased to 57.4% (Harris Poll #12059). Preliminary findings from focus group research, conducted with the sponsorship of the Markle Foundation during 2000, reinforced this apparent ambivalence (Clausing, 2000a). On the one hand, the participants "seemed to trust business over government to regulate the Internet" and "absolutely wanted no government involvement." However, "on privacy and fraud, they echoed the call of buyer beware" and also "seemed to expect some type of rules or protections" enforced by government. The responses clearly underscore the ambivalence that people have about the role of government.

### *2.5. Trust in government: data collection and record-keeping*

Evidence of declining levels of trust in government concerning assurances of confidentiality were recorded between 1968 and 1976 in a series of questions about whether the Census Bureau, Internal Revenue Service, and Social Security Administration would protect personal information (Harris Polls #1815, #7483, and #7680). Although a large majority believed government assurances that their information was secure, the percentage of respondents who did not believe their personal information would be protected grew from 17% to 26% for tax information, from 13% to 15% for census information, and from 7% to 13% for earnings information.

Further declines in trust in government were recorded during the 1980s until mid-2000. When asked, in September 1983, if "a government in Washington will use confidential information to intimidate individuals or groups it feels are its enemies," more than 85% of the leaders and general public responded positively (Harris Poll #832033). Government databases posed a "very serious" or "fairly serious" threat to individual privacy for a majority of respondents (56%) in 1985, and this threat climbed to 78% in 1996 according to the National Opinion Research Center (1996) surveys.[7] A Pew Research Center (2000) survey on trust in government conducted in July 2000 shows a precipitous decline in the level of confidence that personal information will remain confidential even with government assurances. The survey found that only 40% of those surveyed said they could trust their government "at least most of the time."

An April 1997 Harris survey found that 75% of respondents who were computer users opposed local and state governments "putting public records, including real estate, court, and license information, onto the Internet, for easier access by all interested parties" (Harris Poll #738226). Three years later, in 2000, a study directed by Alan Westin, "Public Records and the Responsible Use of Information," found that 84% of respondents "said that government agencies should not be able to display even public records of personal information over the Internet" (McGuire, 2000a). At the same time, however, concern about misuse of their personal information was balanced by more than 60% of these same respondents who would be "comfortable with allowing agencies to post public records if the agencies in question adhered to certain privacy guidelines" and the "nearly 70% of them

who would permit the posting if the agencies in question sought permission from individuals before the fact."

### *2.6. Summary*

Overall, public opinion surveys over more than 30 years show that beliefs about the loss of personal privacy are associated with the quantity of personal information collected by government and the private sector. Computer technology has reinforced the anxiety. Recent increases in concern about personal privacy can be traced to the developments in e-commerce and matters related to consumer protection and are also associated with the sale of personal information, identity theft, and breaches of security in database systems. Americans lack confidence in business practices. People believe that their personal information can be misused or abused and easily exchanged via computer and that they cannot trust the government or the private sector to safeguard their personal information. They support stronger privacy protections for personal information held by the private sector but remain ambivalent about whether government should regulate the private sector.

Public attitudes towards government have had indirect but cumulative effects on support for government record keeping. These attitudes sensitized government agencies to external threats to the social science enterprise might pose and subsequently affected access by the social science community.

## 3. Transformation of government and social science

The expansion of government responsibilities for ensuring the social welfare of the nation that took place during the 1960s and 1970s led to rapid growth in administrative and statistical records. Administrative programs required personal information, and policies and programs required statistical data for monitoring and evaluation.

Computer technology became critical for managing governmental operations and transformed the information infrastructure of government agencies. Enhancements to government administrative record-keeping systems made possible efficiencies in large-scale data collection and processing. Computer matching became a standard administrative tool to investigate fraud, abuse, and mismanagement (Oversight of Computer Matching, 1982). Agencies routinely produced and distributed public use summary data tabulations and microdata files.

Computer technology became equally essential for the operations of the private sector for efficient information management and collection of enormous quantities of personal information. Computer technology was also instrumental in improving the capabilities of the scientific community by providing the computational resources to link survey and administrative records and to organize, manage, retrieve, and analyze large quantities of data (David & Robbin, 1989, 1990; Robbin, 1995; Robbin & David, 1988).[8]

Computer technology was, however, an indispensable but "double-edged sword." While essential for managing the work of government, the private sector, and research in the social scientific community, the widespread use of these sophisticated data practices significantly

contributed to public anxiety about personal privacy and ultimately eroded researchers' access to government statistical and administrative records.

### *3.1. The effects of law and policy on researcher access to government records*

The social research community had historically enjoyed a special relationship with government, one that permitted researchers extraordinary access to administrative and statistical records based on their potential contribution for solving social problems.[9] By the 1960s, social science had become increasingly dependent on data from administrative agencies' statistical record-keeping systems, and the wide array of social program experimentation and evaluation that took place as a result of Great Society initiatives depended on access to such information (Riecken & Boruch, 1978).

The privileged access of the social research community to government information was, however, irrevocably altered by the mid-1970s, a result of a series of court cases and federal and state government intrusions into private lives that clarified the failure of existing laws to protect informational privacy.[10] Public anxiety about the loss of privacy, government databanks, and computers, reinforced by congressional hearings and the media, fueled the implementation of federal and state statutes, regulations, and administrative policies and guidelines to safeguard privacy and create enforceable expectations of confidentiality.[11] Threats to personal privacy by computer technology, government, and the private sector were widely popularized (e.g., Flaherty, 1979, 1989; Sieghart, 1976; University of California at Los Angeles, Law Review Research Project, 1968; Westin, 1971, 1976a, 1976b; Westin & Baker, 1972).

The nature of public support for science and technology also changed, moving from advocacy to questioning the nature of the research activity (Weingart, 1982; Wulff, 1979). Government began to intervene through regulation and public policy to intrude into science's traditional autonomy.[12]

The Privacy Act of 1974 and other statutory controls on access to identifiable records were especially effective in modifying the relationship between the social research community and government agencies. The Privacy Protection Study Commission subsequently recognized these potentially detrimental effects. By the latter half of the 1970s, government officials who supported research on government records and members of the research community began to register concern that the Privacy Act and confidentiality provisions in other statutes had unintentionally and detrimentally affected access to data for research.

For example, Jabine (1975, p. 229), at the time a member of the Social Security Administration, wrote that, "Over the long term, the Privacy Act [could] be expected to reduce. . .the amount and kinds of statistical data, which the [Social Security Administration's] Office of Research and Statistics [would] be able to provide both for internal SSA purposes and for outside users. The data. . .will be less timely and of poorer quality." Hulett (1977, p. 207), another government official, noted that, "It [was] not unlikely that agencies [would] take a narrow view of appropriate uses of their data, thereby unduly restricting statistical or research activities, which serve broader public purposes." Indeed, by the late 1970s, government agencies like the Social Security Administration and the Internal Revenue

Service, which had once provided public use or restricted access files to university researchers, terminated the production and distribution of public use files that had been available to the research community for more than 10 years.[13]

The Privacy Protection Study Commission (1977) also concluded that as research and statistical activities became more dependent on administrative records, it had become more difficult for individuals to "control the way information about [them was] collected and used" (p. 568). The growing amount of research and statistical activities "called into question the validity of the expectation of confidentiality." Moreover, the "use of individually identifiable research and statistical records for administrative, regulatory, or law enforcement purposes encourage[d] abuse of the expectation that information will be kept confidential" (p. 568). The Commission recommended that a "clear boundary be established between the use of such information and the use of information that is collected, maintained, or disseminated for other purposes" and that the principle of "functional separation" be adopted to "functionally separate" federal agency research and statistical activities from policy and decision-making units (p. 572). This principle would be enunciated by government and private sector researchers and statisticians over the next two decades and would serve as a cornerstone for recommendations governing statistical practices and the use of administrative records (see Duncan et al., 1993, pp. 4–6, 34–35, 53–54, and 217–218).

During the development of privacy and confidentiality laws, members of the statistical communities and governments in western Europe, Canada, and the US initiated a series of policy reviews and analyses (American Statistical Association, 1977; Clark & Coffey, 1984; Dalenius, 1979; Dalenius & Klevmarken, 1976; Durbin, 1979; Duncan et al., 1993; Fienberg, Martin, & Straf, 1985; Flaherty, 1978; Hedrick, Boruch, & Ross, 1978; Hewitt, 1979; Martin & Straf, 1992; Mochmann & Müller, 1979a, 1979b; Spruill, 1984; U.S. National Research Council, 1979, 2000; U.S. Office of Federal Statistical Policy and Standards, 1978a; U.S. Privacy Protection Study Commission, 1977; Wilson & Smith, 1984). Government and other statisticians made significant progress in assessing statistical disclosure risk and in developing statistical techniques and administrative procedures for controlling risk. Government inter-agency committees published the results of these studies (U.S. Office of Federal Statistical Policy and Standards, 1978b). Other groups and investigators examined the effects of confidentiality/privacy statutes and administrative policies on the social research process (Gordon & Heinz, 1979; Robbin, 1981, 1984; Sasfy & Siegel, 1981a, 1981b).

Researchers conducted controlled experiments to test methodological approaches for assuring the confidentiality of social research data. Field experiments examined the effects of wording of informed consent statements (Boruch, 1979; Boruch & Cecil, 1979, 1983; Singer, 1978, 1983; U.S. National Research Council, 1979). The underlying rationale for this research was the potential negative consequences of citizen refusal to participate in government record-keeping activities. High participation rates in the decennial census, government surveys and, more generally, administrative record keeping were viewed as essential for the functioning and maintenance of the political system. Citizens supplied information that was necessary for designing, monitoring, and evaluating public policy. Participation in government surveys was also an indicator of support for government, more

generally, and "full and accurate information from individuals and households" required that government agencies had the respondent's trust and cooperation (U.S. National Research Council, 1979, p. 1).

In sum, beginning in the early 1970s, legislative initiatives and agency policies on privacy and confidentiality played a critical role in altering the relatively easy access to government records that social scientists had enjoyed in earlier decades. These developments stimulated important theoretical research in statistical disclosure risk and methodological research to improve the confidentiality of research data. All the same, social scientists did not operate in a vacuum. Public opinion about privacy and confidentiality had played a critical role in defining the legislative agenda, in developing statistical agencies' policies, and in stimulating these social scientists' basic research activities to understand the consequences of privacy concerns for participation in government record-keeping.

## 4. Privacy concerns and participation in the decennial census

Declining participation rates in the decennial census, from 78% in 1970 to 65% in 1990, were an impetus for federal government research on privacy concerns. For example, after the 1990 decennial census, the National Opinion Research Center conducted a Survey of Census Participation (SCP) to ascertain reasons for census nonresponse (Martin, 2000; Singer, Mathiowetz, & Couper, 1993). Confidence in the Census Bureau's assurances of confidentiality had an effect in 1990: 86.1% with high confidence but only 73.5 with low confidence returned their census forms (Singer et al., 1993, pp. 467–468). The researchers found that, overall, privacy and confidentiality concerns affected mail return rates for a small but significant percentage of citizens and that the "crucial variable appears to be trust in the integrity of the data collection agency, not the nature of the assurance given to respondents" (Singer et al., 1993, p. 479).

The decennial census again became controversial in the 2 months leading up to the 2000 census. Critics deemed the long form's questions as too intrusive and too personal. For example, Bast (2000), CEO of the Heartland Institute, a nonprofit policy think-tank advocating free market principles and recipient of the long form, accused the Census Bureau of exceeding its authority and conducting an "unwarranted invasion of privacy." He posted a "Census Workers Not Welcome Here. Do Not Knock" sign that was widely distributed. Census Bureau Director Kenneth Prewitt showed the sign at a June 10, 2000 news briefing to illustrate the "organized resistance" that the Bureau continued to face (Census, 2000a).

Public perceptions that the Bureau could not be trusted were confirmed when the national media reported on the Census Bureau's participation in the internment of Japanese Americans during World War II (Holmes, 2000a; Seltzer & Anderson, 2000). Although the Bureau did not supply names and addresses of people of Japanese ancestry to the Defense Department, it provided information about their concentrations in small geographic areas. This "news" was, of course, not new, although the Bureau did not publicly acknowledge its role until 1981 (Roth, 1981). Nonetheless, the "revelation" occurred when the Bureau was about to field the 2000 census. It also raised fears among ethnic groups with high levels of immigration, like

Latinos, that census data could be used to arrest illegal immigrants. It also coincided with alleged breaches in national security by a Chinese American scientist that contributed to a continuing hostility against the "foreign presence" of Asian Americans (Glanz, 2000; Kang, 2000; Norman, 2000a). To make matters worse, the national press reported that the Census Bureau had been communicating to new employees a "false account of [its] handling of confidential material in World War II" (Norman, 2000b).

Politicians of all political persuasions weighed in with press releases. From the floors of Congress, both Republicans and Democrats intoned their opposition to government bureaucracy, excusing their constituents from completing the census form. Representative Nick Smith (R-MI) complained that, "There are too many curiosity questions on the Census long form. Right now. . .citizens are asked. . .very personal questions, very intrusive questions. . .I think. . .the danger is a government that, out of curiosity, would like to know more than they really need to know about our individual lives" (Smith, 2000, p. H1418; see also Rosenbaum, 2000). Representative James A. Traficant (D-OH) accused the Census Bureau of "literally [being] out of control" and went on to say:

> Check this out: Reports now say that the Census Bureau is, quote/unquote, willing to sacrifice a true head count of American citizens for more personal detailed information. Unbelievable. Forms with questions about your bank account, your cars, how many bathrooms you have, your job. What is next, Congress, your sex life? The Constitution mandates a simple head count by a Census taker, not an audit by some bureaucratic intrusive nincompoop. I yield back the manipulations of both American citizens and our great Constitution by the Census Bureau (Traficant, 2000, p. H1419).

Census Bureau Director Kenneth Prewitt, at news conferences, in testimony before congressional committees, and through press releases, repeatedly explained that every question on the census "was put there to fulfill some very serious piece of legislation or government program" (Rosenbaum, 2000). The Census Bureau's rapid response and an explanation of the relationship of the census to intergovernmental revenue transfers to the states clarified the effects of nonparticipation. Congressional opponents eventually issued press releases that encouraged their constituents to complete the census. Senate Majority leader Trent Lott (R-MS), for example, while noting the "intrusive" nature of census questions, emphasized the importance of the census for "Mississippi's future":

> I urge that all Mississippians respond to Census 2000. Since 1790, the census has determined the number of Congressional seats allotted to each state. Today, it also helps determine how much of your federal tax dollars will return to your community. If Mississippi's census participation doesn't improve, Mississippians will be short-changed in both areas — possibly losing an estimated US$400 million in federal funds, and one of five Congressional seats. . .Many Mississippians have called my office objecting to what they deem are intrusive questions on the census "long form," which about one in seven households received. If you feel you cannot answer a question, please don't throw the form away. Federal law requires us to fully answer the census and ensures confidentiality. However, if you feel you cannot answer a question, please call the main census help line at 1-800-471-9424. The census is just too important to our fellow Mississippians to simply be discarded. . .Census 2000 is Mississippi's future. Please don't leave it blank (Lott, 2000).

InterSurvey, a survey research firm, confirmed the political damage to the Bureau by following a national sample of Americans as part of its research on exposure to Census 2000 advertising (Nie, Junn, & Slotwiner, 2000). InterSurvey conducted a survey with a separate sample of nearly 2000 persons the week following negative media coverage of the "long form" to determine whether the controversy over the long form had influenced participation rates (Nie & Junn, 2000). The survey indicated that privacy concerns increased from about 10% at the beginning of March to 20% by mid-April. The researchers found that household participation rates differed significantly between people who saw the census as an invasion of privacy and those who did not. The controversy decreased participation: 9% were less likely to participate, 48% less likely to answer all long form questions, and 29% less likely to answer all short form questions (Nie et al., 2000, Slide 19). Eighty-four percent of those who had received the long form viewed the income and physical and mental disabilities questions as too personal (Nie et al., 2000, Slide 20). However, InterSurvey also found that exposure to the Census 2000 promotion and mobilization effort increased participation, even for people with privacy concerns, thus confirming that the Bureau's mobilization through advertising could mitigate some of the damage done through linkage of privacy issues to participation in the decennial census.

The long form controversy also reinforced public concerns about the availability of personal information through the Internet. As one person commented to a newspaper reporter, "There is enough information out there on every person walking this earth. . .All they have to do is get somebody with a Pentium III and hook up to the Internet and they would get everything they want. They do not need a census organization" (Norman, 2000b). The public furor over privacy and computer security so sensitized the Census Bureau that the agency maintained a low profile about how citizens could complete the "short form" online at the census Web site (Hammer, 2000). Finally, the Bureau also could not ignore that privacy and confidentiality concerns had interacted with the long-standing controversy over statistical adjustment, sampling, and the accuracy of the census (Holmes, 2000b, 2000c, 2000d), the well-publicized "screw-up," as Congressman Jack Kingston (R-GA) put it, of sending out a preliminary notice of the arrival of the census form to incorrect mailing addresses (Kingston, 2000, p. H10831; Myers, 2000), and that its funding for completing Census 2000 operations was not yet secure (Census 2000b, 2000c).[14]

### *4.1. Census Bureau response: access to the 2000 PUMS and consequences for social research*[15]

From 1790 to 1950, the U.S. Bureau of the Census published decennial census tabulations by geographic area. In 1960, in what demographer Steven Ruggles, director of the Minnesota Population Center at the University of Minnesota, has called a "paradigm shift," the Census Bureau created and disseminated a 1-in-1000 extract of the complete enumeration, which was released as a PUMS.[16] Ruggles wrote that the 1960–1990 PUMS, along with the 1940 and 1950 1-in-100 samples produced at the University of Wisconsin-Madison, "revolutionized the analysis of the American population," led to "an explosion of census-based research," and established PUMS as "the mainstay of American social science" ("Background and

Significance," p. 1). What made the PUMS data so important, Ruggles noted, were their "broad chronological scope, large sample populations, and fine detail" ("Background and Significance," p. 1).

Individual-level sample data from the decennial census can be released because the Bureau deletes names, addresses, and "other potentially identifying information" to protect the confidentiality of respondents. Detail on geography is limited to the areas with more than 100,000 population.[17] The Bureau also applies rules to protect individual identification for geographic location of residence and work, income, and several other variables.[18] Decisions regarding subject detail and geography were a result of significant, previously noted research in assessing statistical disclosure risk, reidentification of respondents, and developing confidentiality-preserving statistical methods by statisticians at the Bureau of the Census and elsewhere (Fienberg & Willenborg, 1998; Kim & Winkler, 1997; U.S. Federal Committee on Statistical Methodology, 1994, 1999; U.S. Office of Federal Statistical Policy and Standards, 1978b; Winkler, 1997, 1998, 1999).

In mid-Spring 2000, reacting to congressional criticism about statistical adjustment (Anderson & Feinberg, 1999; Skerry, 2000) and the public controversy over the long form, the Census Bureau proposed significant reductions in the level of subject detail for the 2000 PUMS to "reassure" citizens about the Bureau's commitment to preserving confidentiality. The response by the social science community to the Bureau's proposal was swift. The Inter-University Consortium for Political and Social Research (ICPSR) at the University of Michigan organized a "Task Force on the 2000 PUMS" with the goal of "proposing a balance between data integrity and issues of confidentiality" ("Why Is There a Task Force?"). On May 9, 2000, demographer Richard Ruggles, who served as chair of the ICPSR Census 2000 Advisory Committee, distributed a letter over the Internet that described the Bureau's plans, stated that he would be attending a Bureau-sponsored "Census 2000 Users Conference on PUMS" on May 22, 2000 that was designed to "gauge the reaction of the user community to the proposed changes" and requested that concerned PUMS users complete a user survey ("Appendix A. ICPSR Letter and Survey").

The letter received wide circulation. Professional listservs and associations served to mobilize demographers, historians, and social scientists. More than 1000 people in the academic and policy communities responded to the Web-based survey on the importance of the PUMS data ("Design and Execution"). The Task Force published the results of the survey in a detailed report entitled, "The Public Use Microdata Samples of the U.S. Census: Research Applications and Privacy," which was communicated to the Census Bureau at the May meeting.

The Task Force's preliminary analysis of the Bureau's proposal indicated that the "impact of [the proposed] Bureau plan would

- group ages into 5-year categories for persons aged 65 or older and reduce the top code for age from 90 to 85,
- reduce the number of ancestry categories from 560 to 105,
- reduce the Hispanic origin categories from 206 to 23,
- reduce the number of identified occupational groups from 505 to 67,
- reduce the number of identified industry groups from 244 to 70,

- reduce the number of language categories from 393 to 83, and
- eliminate 298 foreign countries of birth and substitute 14 continents and US possessions" ("Summary").

Subsequent analysis suggested even more troublesome Bureau decisions. In a June 2 listserv update to PUMS users, Task Force Chair Ruggles remarked that a number of Bureau classifications "did not seem to make much sense," appeared "to be hastily conceived with no systematic underlying principles," and had "no scientific basis" (Ruggles, 2000a). For example, the Bureau proposed to "collapse very large occupational groups, such as teachers, construction trades, and motor vehicle operators into single huge categories but to maintain small occupational groups like librarians and archivists." Certain occupations like childcare workers "would no longer be identifiable." Moreover, foreign countries of birth would not be identified (item on ancestry). However, "in some cases, extremely small groups" would be identified, such as American Indian tribes and members of US possessions. The report identified anomalies, including recodes that "appear[ed] arbitrary and unsystematic (e.g., Shoshone Native Americans and persons of Albanian descent [would] be identified but not persons of Mexican or Chinese birth)" ("Conclusion and Recommendations").

The Task Force's report was a powerful affirmation of the value of releasing government data and how influential a tool the PUMS data files have been for the creation of new knowledge and for public policy. It was immediately apparent that reductions in subject detail and geography would curtail, eliminate, or significantly jeopardize important ongoing and future research. For example, the report noted that, "concern had been expressed about geography, income, and age variables," but "approximately 90% of faculty researchers also said that a reduction in the detail available on occupation and race would have 'catastrophic' or 'very harmful' consequences for research in their field" ("Results").

The richly textured qualitative responses to questions about the effects of reductions of PUMS subject and geography detail identified by professional demographers, social scientists, historians, and policy analysts and the emerging generation of scholars who are currently graduate students told a compelling story ("Appendix C. Reduction of PUMS Detail and Your Research"). The key question in the survey that elicited an extensive exposition of the utility of these data was "Please comment below on ways in which reduction of PUMS detail might affect your research. Be specific as possible. For example, if you specialize in aging research, comment on the sorts of analyses that would be precluded by grouped age data." The "Results" section of the Report summarized some of the principal arenas in which current social research is carried out.

> We had hundreds of responses to this inquiry. . .Many respondents focus their research on particular population subgroups, which they might be unable to identify in a less-detailed sample. Some examples include studies of immigrant groups within metropolitan areas, the changing demographics of hotel and restaurants workers in San Francisco and Los Angeles, the legal profession, and specific Asian-Pacific populations. Policy makers in particular expressed concern about the loss of the detail needed to study issues such as school voucher programs, welfare reform, residential segregation, urban poverty, and measures of social and economic inequality at the local level ("Survey Results").

The Bureau was asked to "avoid making precipitous decisions that [would] do permanent damage to social science research in the US" ("Summary").

### 4.2. Seeking explanation for the Bureau's proposal: politics and information privacy

Many respondents linked the Bureau's proposal to a hostile political environment, public controversy over the long form, media coverage, and privacy concerns by a worried citizenry that were more appropriately targeted at the e-commerce private sector.[19] A faculty member commented, "This move to limit detail sounds like a knee-jerk reaction to the pseudo-fuss last month over 'invasive' long form questions." Another respondent wrote, "To the best of my knowledge, 2000 is the first census year in which there has been so much media coverage devoted to any sort of privacy concerns related to census data. If not for said media coverage, I doubt this would even be an issue." A researcher commented,

> It seems that the real interest in limiting the data has little to do with confidentiality and much to do with saving money and promoting a political agenda. The whole anti-census issue seems a political ploy to rally public opinion against 'big government' by attacking a relatively defenseless target, meanwhile limiting the ability of pesky social science researchers to ask important and difficult questions.

The Bureau's proposal was not an appropriate response to the public's concerns about privacy, respondents asserted. The concern about privacy "needs to be directed at its true source, private sector Internet businesses, and [not] redirected at academic researchers who would have no interest in trying to identify individuals."

Respondents compared the release of anonymized PUMS detail to the quantities of easily accessible personally identifiable information that private sector firms maintain on individuals and access to databases on the Web. One person commented that it "amazed" him that "people who will happily allow unknown corporations to track their Internet reading, electronic shopping behavior, and spending patterns are worried that egg-heads like myself will try to find out where they live." Another person contended that, "There is no information in the PUMS that I can conceive of anyone wanting for inappropriate reasons, which could not be found more easily from credit reporting agencies and other administrative sources." A faculty member recognized "the concern" and was "appalled by the loss of privacy in the age of linked computer records and the Internet." However, he continued, "It seems quixotic to worry about privacy in Census data when marketers and geodemographic companies combine to know more and more about individuals. I worry more about my medical records being in the hands of my employer."

The general assessment was that people disclosed "far more identifying information about themselves in the course of surfing the net than they do in filling out the long form." Furthermore, "unlike academic researchers, Internet companies and Web site developers are not constrained by professional codes of ethics or institutional rules against profit mongering." A graduate student wrote that, "I cannot really imagine how people would use the PUMS to get access to information about specific people. There are so many more real threats to privacy embedded in the proliferation of online databases accessible through the Web."

Over and over again, respondents rejected the notion that it was possible to identify individuals from the sample data. One person commented that, "Someone would have to work *very* hard to reveal odd cases that stand out in the data. Given that only 1 in 20 cases will be released, census data are a much less effective means of discovering private information about specific individuals than recourse to privately maintained databases that even include exact names and addresses."

PUMS users concluded that individual identification was not an activity that any scholar was interested in pursuing and that "concerns about the confidentiality of PUMS data are vastly overstated." They also questioned the logic of reductions in subject detail without empirical evidence to demonstrate that disclosure had actually occurred. One person asked rhetorically, "Given that there has never been a breech of confidentiality privilege in the use of PUMS, why is it necessary to make any changes?" Indeed, the assessment of the Task Force was that, "In the 36-year history of the census microdata samples, no respondent has ever been identified by anyone outside the Census Bureau. We consider such identification to be highly improbable even under the current standards" ("Summary").

Ruggles's (2000a) June 2, 2000 update of "PUMS 2000 News" affirmed that the Bureau had "legitimate concerns about congressional criticism of the long form." However, he went on to say, "Haphazard and excessive reductions in the detail available to scholars and planners will do little or nothing to protect respondent confidentiality." He pointed out that the Bureau's "fears about respondent disclosure" were based on faulty reasoning about the outcome of linking summary and sample files, because confidentiality edits had already been applied. He contended that the proposed "reductions in the subject area detail would not ameliorate the risk posed by linking in the slightest, since even under the Bureau's plan the PUMS will still include as much subject detail as do the summary files."

Nonetheless, the Report acknowledged that the Bureau had legitimate concerns and that there were political reasons for reducing the possibility of disclosure. "Privacy in America is indeed under assault," and thus the public needed to be reassured that "the risk of disclosure is negligible" ("Summary"). The recommendation was to close the "gaps in the confidentiality safety net" for "some census categories whose cell size was too small in the 1990 PUMS," which "may pose at least a theoretical, if not a practical, risk of disclosure" and could be "accomplished by reducing the minimum population threshold to 10,000 or 25,000 persons for every sensitive census category." While the recommendation would mean a "radical change" that "would doubtless be opposed by some researchers," the Report suggested that, "it was a better solution than the one proposed by the Census Bureau." The report also recommended that the "one remaining confidentiality gap" be closed by suppressing the PUMA codes in the summary files for sample persons who appear in the PUMS.

The responses to the survey also underscored the continuing debate regarding the balancing of the principles of personal privacy and data sharing — and the privileging of the value of access, which would be expected from the scholarly community. One respondent captured this point of view, which was expressed by all respondents: "Restricting access or eliminating important information does not serve the broader purposes of collecting such data — better understanding of social conditions and problems, information about the effect of

public policies on social conditions, and insights into how to improve matters." From Paris, France, a researcher wrote to say that, "Please stop with confidentiality paranoia: ethics and deontology of information is not simply a question of individual confidentiality but a balance between individual confidentiality and sociostatistical knowledge."

### *4.3. Postscript: the Bureau responds*

On November 6, 2000, Ruggles (2000b) wrote to the PUMS listserv that, "I am happy to report success in our efforts to preserve needed detail in the 2000 PUMS. . .The Census Bureau took our concerns seriously [and] adopted all the principal recommendations of the Task Force."

The Bureau of the Census issued its "Recommendations Concerning the Census 2000 Public Use Microdata Sample (PUMS) Files" in October 2000 (U.S. Bureau of the Census, 2000). The Bureau affirmed that its proposal to modify the 2000 PUMS was directly related to privacy concerns. It contended that "rapid advances" in computer technology had made it "more difficult. . .to protect the confidentiality of microdata through disclosure limitation techniques," and, as such, it had been necessary to "strengthen the confidentiality protection that we provide for microdata files" (p. 1). The Bureau identified threats related to the computer as "more powerful computers, greater data storage capacity, increased access to the Internet, and advances in data linking and data mining" (p. 1). Privacy concerns had to be balanced with the needs of users, and we listened, wrote the Bureau.

As such, the Bureau's recommendation called for issuing two sets of PUMS files: 5% state files and a 1% national characteristics file. The "possibility of disclosure problems" had already led them to implement data swapping and top-coding methods.[20] State-level files would contain information for "most metropolitan areas (i.e., 231/276 or 84%) and the more populous counties and central cities" with a minimum threshold population of 100,000, and variables would be collapsed "to the level deemed necessary to maintain confidentiality while retaining the current threshold" (p. 1). The Bureau acknowledged that this threshold was the minimum necessary for "studies by public agencies, academic researchers, and the private sector" and acknowledged that to increase the threshold to 250,000 would reduce to 50% the number of metropolitan areas "that could be recognized" (p. 2).

The objective of the national characteristics file was to "achieve as much as possible the amount of detail that was provided in the 1980 and 1990 PUMS files" (p. 3). The PUMA would have a minimum population threshold of 400,000. The Bureau was committed to minimizing the number of variables that would be collapsed in order to "maximize the amount of social, economic, and housing information available" (p. 3). As such, there were no plans to establish a minimum population threshold on variables.

Limits would be established on the detail of certain variables.

- Dollar amounts would be rounded and applied to all income types' dollar amounts, utility costs, mortgage costs, rent, condominium costs, and mobile home fees.
- All categories of race and Hispanic origin would appear on the 1% file. However, only categories with at least 10,000 population would appear on the 5% files.

- State- and national-level files would contain single-age categories 0–89 and be top-coded at 90. Large households, defined as 10 or more persons, would be masked in the state-level files. However, large households would receive a state identifier but not a PUMA identifier.
- Travel time would be treated as a continuous variable with top-coding but no other collapsing or rounding, but departure time would be rounded (p. 5).
- Year of entry would be bottom-coded in direct relation to the top-coding for age (p. 5).

A minimum population threshold of 10,000 within categorical variables would be maintained to permit identification of groups. Rather than predetermining which variables or how to collapse the categories, the Bureau would evaluate the records and "user input" would be sought "to find the most meaningful combinations of variable categories" (p. 2). Thus, what marked a significant change from past Bureau decision-making was that the user community would be consulted about how public use data files would be released. Their advice would be sought on the types of analyses to be carried out and the criteria to be used "to collapse categories that did not meet the 10,000 threshold in the state-level files" (p. 6).[21]

The Bureau would not, however, issue any national metro files for populations of 100,000 or more, similar to what was issued in 1990. The possible combinations of national, state, and metro public use files either did not satisfy the Disclosure Review Board's limitation on total sample density of no more than 6% or were unsatisfactory to users because the sample density was insufficient or the detail was reduced.

In sum, the Bureau's efforts were designed to protect the twin principles to which it has traditionally been committed. The PUMS files would ensure the confidentiality of records and provide data for scientific discovery and informed public policy.

## 5. No place to hide any more

The debate about the release of microdata public use files took place in an environment where tensions between privacy and access have grown markedly over the last three decades. The controversy over the 2000 census long form, deemed intrusive by some members of Congress and many citizens, coupled with widespread knowledge that private sector firms and government agencies collect, use, and sell personal information, heightened public concerns about information privacy and led to growing support for improved statutory protection of individually identifiable government and private sector information.

Personal information became a lucrative commodity for government and the private sector (Allen, 2000; Bunn, 2000; Chandrasekaran, 1998; Clausing, 2000b, 2000c; CNET News.com, 2000; Peterson, 1997; U.S. Federal Trade Commission, 2000; Weinstein, 1997, 1999). Government agencies and private sector firms carry out Web site surveillance to monitor usage, and private sector firms collect and use personal information of visitors to their site for other purposes (Clausing, 2000d; Keizer, 1997). State and local governments and e-commerce companies sell personal information, often without the customer's

permission (Bernstein, 1997a; Clausing, 2000c, 2000d, 2000e; 2000f; Kang, 1998; Keizer, 1997; O'Harrow, 1998; U.S. Federal Trade Commission, 1998). Much of what takes place, whether its collection, sale, or manipulation, is unknown to the consumer (Treese, 2000). "People are losing control over their own identities," said Senator Dianne Feinstein (D-CA) (Bernstein, 1997b).

Threats to personal privacy seem unending, as witnessed by a recent report that the caches of Web browsers create a threat that "allows nosey unscrupulous Web site operators to spy on their visitors' browsing habits" (Austen, 2000). Geographic tracking systems trace Internet addresses and are used to locate target audiences for Web sites and advertisers (Olse, 2000). Advances in wireless technology provide an opportunity for businesses to monitor their employees and consumers (Savage & Stirpe, 2000). E-commerce firms are developing systems to "vastly improve their ability to share names, identification numbers, and a wealth of behavioral data about individual consumers" (O'Harrow, 2000). There is no place to hide (Johnston, 2000; Koppell, 2000; Privacy Foundation, 2001). Along with these developments have also come well-publicized technology failures. Breaches in the security of, as well as recent attacks on, business, university, and government e-mail systems, medical and health databases, and Web sites, have intensified fears (Lohr, 1997; Markoff, 2000; Naylor & Upton, 1999; Okie, 2000; Omega World Travel, 2000; Rubin, 2000; Schneier, 1999; Seminario, 1998; Upton, 1999).

Institutional policies and practices have altered the relationship between government and citizen, between government and the marketplace, and between the individual and the marketplace. The array of organizations that "claim a stake in" confidentiality and data access issues has increased (Duncan et al., 1993, p. 54). Only witness the latest threat to Title 13 that undergirds the confidentiality assurances made by the U.S. Bureau of the Census. In late 2000, the Congressional Budget Office (CBO), with support from congressional Republicans, requested access to census bureau files to create a linked data set using information from Internal Revenue Service, Social Security Administration and Census Bureau surveys that would "help CBO evaluate proposed reforms in Medicare and Social Security" (Monk, 2000). The spokesman for Representative Dan Miller who chaired the House subcommittee on the census "saw no problem with congressional access to census data" because "the Census Bureau is the government and Congress is the government."

Personal information has become mediated by a private sector that operates under different legal mandates from government agencies. Private organizations increasingly assume responsibility for data collection and dissemination. In the process of "reinventing government," government agencies have outsourced responsibilities for program implementation, including program eligibility determination, billing, check cutting, quality control, and client auditing and accountability. Computerized information systems, formerly the responsibility of government agencies, are now operated by data brokers.

There is no consistent set of statutes or regulations for administrative or statistical records that governs all federal agencies or provides guarantees of confidentiality, either for government or for the private firms that now administer government programs. Statutory protection is weak or nonexistent for the private sector.

### 5.1. Congressional responses

As public concern mounted, a number of hearings were held during the first session of the 106th Congress on protecting consumer information maintained by financial institutions, protecting the confidentiality of medical records, and protecting privacy in the conduct of research in genetics and medical research more generally (Financial Privacy, 1999; Genetics Testing in the New Millennium, 1999; Medical Information Protection and Research Enhancement Act of 1999, 1999; Medical Records Confidentiality in a Changing Health Care Environment, 1999; Medical Records Confidentiality in the Modern Delivery of Health Care, 1999; Medical Records Privacy, 1999; Privacy Under a Microscope, 1999). Congressmen spoke from the floors of Congress about the loss of personal privacy, condemning "today's information society" (Hutchinson, 2000, p. H1288). However, only two major pieces of privacy legislation were enacted. The Children's Online Privacy Protection Act of 1998 (P.L. 105-277; 15 USCS §6501) required Web sites to obtain parental permission before personal information could be requested from children under 16 years (Children's Online Privacy Protection Rule, 1999; Clausing, 2000e, 2000f). More likely of greater consequence for consumers was the enactment of the Financial Services Modernization Act of 1999 (Pub. Law No. 106-102; 13 Stat 1338) governing how financial institutions could collect and share online financial information about their clients; its minimalist approach to regulation met with industry approval (it was deemed "reasonable") (McCullagh & Morehead, 2000).

Bills containing some sort of provision for enforcing online or electronic confidentiality and protecting the privacy of personal information, including customer and medical information privacy, were again submitted during the 106th Congress.[22] Once again, privacy-related bills languished in committee and died at the end of the second session, attesting to the lack of success that privacy advocates had in persuading Congress to support legislation that provided statutory protection against misuse of personal information by the private sector, to protect the privacy of electronically stored medical records, or to monitor e-commerce firms' privacy protections (Clausing, 2000b, Richtel, 2000; Weinstein, 2000).

### 5.2. Executive branch responses

Executive branch initiatives have been a response to Congress's abrogation of responsibility for enacting legal safeguards for personal privacy. Even so, government agencies have been slow to act, responding as Congress did, to pressure from the powerful lobbying efforts of the private sector.

As late as 1999, the Federal Trade Commission (FTC), argued that "voluntary industry practices were working just fine" and that "no legislative action [was] necessary at this time" (Caruso, 1999; Frishberg, 2000; Okie, 2000). The agency's recommendation that the private sector voluntarily enforce itself did, nonetheless, carry the threat of future agency action to protect consumer privacy if changes were not forthcoming (U.S. Department of Commerce, 1999). Eight months later, seeing no progress by industry, the FTC again warned the business and advertising industry "to deal promptly with privacy concerns or

face more legislation,'' leading one member of the Internet Advertising Bureau to attribute the FTC's ''turn-around'' and the response of other executive agencies and Congress to the ''politics of an election year'' (McCullagh & Morehead, 2000). Still, the industry acknowledged, the financial problems and bankruptcies of e-commerce companies like DoubleClick and Toysmart had fueled the information privacy issue with their plans to sell valuable assets, their customer information, to raise money (Stellin, 2000).

The FTC was, however, very serious. In May 2000, after extensive research to determine the extent of personal information held by business and the lack of consumer privacy protections, the FTC recommended legislation that would ''establish basic standards of practice for the collection of information online and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act'' (Pitofsky, 2000; U.S. Federal Trade Commission, 2000). Four months later, the FTC reported the results of a September 2000 review of three US seal programs and ''gave none a passing grade'' (Sanders, 2000).

The private sector's opposition to consumer and employee privacy protection in the US also extended to the comprehensive data protection laws and directives adopted by the Organization for Economic Cooperation and Development (OECD) Council of Europe and Canada, and fair information practices law that is being developed in eastern Europe and Latin America (on international developments, see Pritchard, 2000; Rodger, 2000; The European Commission, 1997). The stakes in these activities are very high for the US because these data protection laws forbid the transfer of personal information to countries without similar protections. Congress's inability to enact similar legislation led the U.S. Department of Commerce to develop a ''safe harbor'' framework to bridge the significant policy differences between the US and Europe. This framework was finally approved by the European Union in July 2000 after 2 years of negotiations (U.S. Department of Commerce, 2000). Companies will be subject to a European Data Protection Commission's ''finding of adequacy'' and ''other benefits'' that will flow from a safe harbor seal of approval. *The Standard*, a now-defunct Internet wire service, commented that, ''Short of negotiating directly with European authorities or physically processing relevant information only within EU borders, American companies will have no choice but to subscribe to the safe harbor, lest they risk losing remote access to European customers, employees, or business partners'' (The Industry Standard, 2000).

Congress' refusal to pass medical privacy legislation led the U.S. Department of Health and Human Services (HHS), exercising its authority under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), to develop regulations that would establish uniform federal privacy protections for personal health information (Markoff, 1998; Pear, 2000a; Standards for Privacy, 2000; U.S. Office of the President, 2000). When the final rules were published in December 2000, they were immediately challenged by the healthcare industry (Pear, 2000b) but were ultimately supported by the Bush Administration.

All the same, public concerns about privacy had already resonated throughout HHS and had had consequences for the release of microdata files. The language of the Act had been interpreted by some HHS agency staff not to permit the release of public use microdata files, and work that had begun ceased shortly after its enactment (Robbin & Koball, in press). Thus,

it is expected that executive branch decisions will have far-reaching consequences for public policy as it relates to the release of government records for social science research.

## 6. Conclusion

Privacy was recently named an "emerging hidden issue" that is "ready to explode onto the American electorate," one that "tests off the charts," according to pollsters (Berke, 2000). Public opinion polls that span more than 30 years make clear, however, that privacy is an issue that citizens have reflected on for a very long time. What they are now experiencing is the sense that personal privacy has been eroded by the computer. There is a widely held sense that the digital environment has transformed daily life, and this transformation has compromised individual autonomy (Lewis, 2000). The more than three decades of congressional hearings are symbolic affirmations of this public concern about privacy and confidentiality.

The public's anxiety is legitimate, as was the Bureau's contention that it was "much more difficult to protect the confidentiality of microdata through disclosure limitation techniques" (U.S. Bureau of the Census, 2000, p. 1). Advances in computer and communications technology have reduced substantially the cost of gathering, processing, and retrieving data and it is relatively inexpensive to develop, maintain, and transfer very large databases containing extensive amounts of individually identifiable and sensitive information. Software routinely monitors Web employee work habits, tracks Web site usage, links information about individuals from heterogeneous databases, and extracts useful information from databases (the "data mining" described in the Bureau's report) (Harmon, 1997; Mosquiera, 2000a).

Nonetheless, congressional inaction, private sector opposition to government intervention, and public opinion that both supports government protection of personal privacy and rejects government regulation of private sector's handling of personal information reflect a society with an inability to resolve conflicting and contradictory goals, as one journalist commented (Bernstein, 1997b). It is a "paradox," wrote another journalist, commenting on the results of the Westin survey of "Public Records and the Responsible Use of Information" (Mosquiera, 2000b). Americans are committed to the principle of individual autonomy that supports information privacy. Yet, Americans are equally committed to computerized access to personal information for what it offers in terms of domestic and international security, management, and wealth that an information economy has brought. We should not have high expectations for comprehensive information privacy safeguards, even if privacy legislation is enacted during the 107th Congress (Akin, 2000; Marsan, 2000; McGuire, 2000b, 2000c).

That little headway has been made in regulating the use of personal information by the private sector should also be understood as Congress's faithful rendition of deeply held beliefs by the citizenry: Government more than the private sector requires regulation. Public concern over information privacy is intertwined with the generalized mistrust of political and other institutions that, ironically, advantage powerful private interests at the expense of citizens' personal privacy.

This regulatory impulse, translated into low levels of trust in government and declining participation or completion rates in the decennial census, is motivation enough for government agencies to view the external environment as hostile and to respond by protecting themselves, to reduce scholarly access to data, and to go so far as to terminate the production of public use files. Thus, while government statisticians and policy analysts support the principle of data sharing, their political world is replete with contrary claims, and everything is, as Alexis De Tocqueville observed more than two centuries ago, "agitated, disputed, and uncertain" (Barber, 1988, p. 19). Under conditions of uncertainty and conflict, what ensures the functioning of the administrative system will be privileged. Politics will almost always trump science.

## Acknowledgments

I gratefully acknowledge Blaise Cronin, Editor-in-Chief Steven Zink, and anonymous reviewers for their suggestions.

## Notes

1. See Westin (1976a, p. 6) for definitions of "privacy" and "confidentiality." Privacy concerns "the question of what personal information should be collected or stored at all for a given social function. It involves issues as to the legitimacy and legality of organizational demands for disclosure from individuals and groups and the setting of balances between the individual's control over the disclosure of personal information and the needs of society for the data on which to base decisions about individual situations and to formulate public policy." Confidentiality concerns "the question of how personal data collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses." Boruch and Cecil (1979, p. 25) add that, "An individual's response. . .is regarded as confidential with respect to others if the information coupled with identifiers will not or cannot be disclosed. . .to anyone else. Information or a physical record containing information is said to be identifiable if it includes names or addresses or other forms of unique identification." Duncan, Jabine, and de Wolf (1993, pp. 22–23) differentiate "informational privacy" from "data protection." Information privacy "encompasses an individual's freedom from excessive intrusion in the quest for information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions, and attitudes will be shared or withheld from others." Data protection is applied to the policies and procedures that are developed to "ensure minimal intrusion by data collection and maintenance of data confidentiality. . .Unlike privacy, however, which is an individual right, confidentiality is not restricted to data on individuals and is often extended to data on organizations."

2. In January 1990 (Harris Poll #892049), Louis Harris and Associates asked a national sample if they agreed or disagreed with the following statement (Q.J2): "If we rewrote the Declaration of Independence today, we would probably add 'privacy' to the list of 'life, liberty, and the pursuit of happiness' as a fundamental right. Do you agree or disagree with the following statement?" Agreement: 78.30%, Disagreement: 19.50%.

3. Louis Harris' data reported here are available from the Institute for Research in Social Science, University of North Carolina at Chapel Hill at http://www.irss.unc.edu/data_archiv/pollsearch.html. Searches were conducted for the period 1960–2000 using the terms "privacy" and "privacy and consumer," and tabular summaries were constructed from the individual question responses. Unless otherwise noted, these surveys are national probability samples of adults 18 or 21 years and older, with sample sizes of around 1500. It is important to note changes in

question wording, because they may have had significant effects on how Americans registered their concerns about personal privacy. The "(#xxxx)" in the body of the text refers to the Harris identification number assigned to the survey.

4. Other surveys for this period include Harris Poll #7680 (January 1976), #2521 (February 1976), and #7687 (September 1976).

5. Between 1982 and 1992, the General Social Survey asked a question with the same wording of a national sample and found that 44.6% were very concerned ($n = 1506$). However, a subsample ($n = 354$) asked the same question in 1982 registered a far higher level of very great concern (69%) for a question with precisely the same wording as the Harris polls. See http://www.icpsr.umich.edu/GSS99/codebook/privacy.htm.

6. For national security matters, see also Smith (1990).

7. The question on databanks was one in a series of questions on the role of government. "The federal government has a lot of different pieces of information about people, which computers can bring together very quickly. Is this a very serious threat to individual privacy, a fairly serious threat, not a serious threat, or not a threat at all to individual privacy?" See National Opinion Research Center (1996).

8. Computer matching operations were also employed by the research community to link records from different systems. Seminal research by government agencies began in the early 1970s, with contributions from members of the Social Security Administration, Internal Revenue Service, and Bureau of the Census. Papers that serve as handbooks on modern record matching theory and applications were published during the 1970s and 1980s (U.S. Internal Revenue Service, 1985; U.S. Social Security Administration, 1973).

9. For a history of the relationship between the academy and government, see Duncan and Shelton (1978) and Lyons (1969). For justification of the utility of social science in social problem-solving, see Federal Government Statistics and Statistical Policy (1982), McAdams, Smelser, and Treiman (1982), U.S. National Science Board (1969), and Weiss (1977a, 1977b).

10. Social research was itself also a target. During the early 1970s, law enforcement officials attempted to obtain the names and addresses of research participants in the "Negative Income Tax" experiments. See U.S. National Research Council (1975).

11. Congressional hearings on computer technology and privacy began in the 1960s and continued over the next decades. Early hearings include Federal Data Banks and Constitutional Rights (1974), Oversight of Computer Matching (1982), Oversight of the Privacy Act of 1974 (1983), Privacy of Medical Records (1979), Public Reaction to Privacy Issues (1979), The Computer and Invasion of Privacy (1966); and U.S. Department of Health, Education and Welfare (1973).

12. Statutes identified conditions for access, types of use, and penalties for disclosure for administrative and statistical records. Confidentiality provisions in federal and state statutes were, however, vague, contradictory, and ambiguous concerning the nature of access for research or other purposes. Statutes generally prohibited the release of identifiable information without the written consent of the individual (e.g., Public Health Services Act, Drug Abuse and Treatment Act of 1972, and almost every state confidentiality statute). Other federal and state statutes normally permitted disclosure without consent to those with a [the statutory language generally employed]: "legitimate interest, some of whom may be researchers or may represent research interests" (e.g., Federal Education Rights Act and Privacy Act, state education, social services, health, and mental health statutes). Disclosure could be permitted for "authorized persons engaged in research on [mental health]," for "audit and evaluation. . .specifically authorized by law," or for "bona fide" research, leaving the agency to determine whether the "project constituted 'bona fide' research within the scope of the regulations" (Boruch & Cecil, 1979, p. 12). Researchers inside an agency would normally have no difficulty in accessing records, and researchers hired by an agency (or deputized for a limited period) would, in principle, have the same access to individually identifiable records as members of an agency. For a summary of state level statutes that were developed during the 1970s, see Robbin and Jozefacki (1982).

13. For example, access was terminated to the "Continuous Work History" and "Longitudinal Retirement History." These data files distributed by the Social Security Administration and Health Care Financing Administration, respectively, were two very important series of data files relied on by economists and others. The author recalls that the Tax Reform Act of 1976 was relied on by government agencies to justify their refusal to provide access to these data files by the social research community.

14. It was not until the end of June 2000 that the House of Representatives gave final approval to a bill (H.R. 4690) that would fully fund the remaining operations, and until the end of July 2000, the bill went to a conference committee to resolve differences in funding levels between the House and Senate.

15. This part of the article is based on the report issued by the University of Minnesota Population Center and the Inter-University Consortium for Political and Social Research, Census 2000 Advisory Committee (2000). References are made to various sections of this report (e.g., "Background and significance"). Demographer Steven Ruggles played a central role in mobilizing the social science community, although the corporate entry of the Report is for a committee he chaired, the Inter-University Consortium for Political and Social Research (ICPSR) Census 2000 Committee. As Director of the Minnesota Population Center at the University of Minnesota, which provides access to an integrated PUMS series (IPUMS), Ruggles was invited to the May 22, 2000 meeting held by the U.S. Bureau of the Census. For the announcement of the formation of the Task Force and other materials circulated by listserv, see listserv keep_informed@hist.umn.edu.

16. The 1960 PUMS was re-released in 1970 as a 1-in-100 sample. For a description of the early PUMS, see U.S. Bureau of the Census (1964, 1972, 1973, 1984).

17. The exceptions are the 1960 and 1970 PUMS, whose population is limited to greater than 250,000.

18. On the effects of applying the requirements of confidentiality in Title 13 of the US Code, see U.S. Bureau of the Census (1993a). The wording for the definition of "income" indicates that the Bureau applied a confidentiality rule to limit disclosure: "In the 1990 census, income amounts less than US$999,999 were keyed in dollars. Amounts of US$999,999 or more were treated as US$999,999 and losses of US$9999 or more were treated as minus US$9999 in all of the computer derivations of aggregate income" (U.S. Bureau of the Census, 1993b).

19. Excerpts of comments are drawn from the Report's Appendices C–E. A large number of the survey respondents are identified by name, status, and institutional affiliation, but this article does not identify them.

20. "Data swapping" is a method of editing the source data or exchanging records for a sample of cases. "Top-coding" sets disclosure limitation on all cases that are "in or above a certain percentage of the distribution into a single category" (U.S. Bureau of the Census, 2000, p. 1, footnote 1).

21. This will particularly affect the race, ethnic group, and ancestry items.

22. These included the Electronic Privacy Bill of Rights Act of 1999 (H.R. 3321), Online Privacy Protection Act of 1999 (S. 809), Online Privacy Protection Act of 2000 (H.R. 3560), the Consumer Internet Privacy Enhancement Act (S. 2928), Medical Financial Privacy Protection Act (H.R. 4585), Medical Information Privacy and Security Act (S. 573, H.R. 1057), and Medical Privacy in the Age of New Technologies Act of 1999 (H.R. 2878).

## References

Akin, A. (2000, November 21). U.S. likely to bring in privacy law. *National Post Online.* Retrieved November 27, 2000, from http://www.nationalpost.com/. . ./2000121/377105.html

Allen, J. (2000, February 2). Sometimes, the Web site is watching you right back. *Los Angeles Times*, p. S1.

American Statistical Association. (1977, February). Report of ad hoc committee on privacy and confidentiality. *The American Statistician*, *31*(2), 59–78.

Anderson, M., & Fienberg, S. E. (1999). *Who counts? The politics of census-taking in contemporary America*. New York: Russell Sage Foundation.

Austen, I. (2000, December 14). Study finds that caching by browsers creates a threat to surfers' privacy. *New York Times.* Retrieved December 20, 2000, from http://www.nytimes.com/2000/12/14/technology/14PRIV.html

Barber, B. R. (1988). *The conquest of politics: Liberal philosophy in democratic times*. Princeton, NJ: Princeton University Press.

Bast, J. L. (2000, July). I can't believe this is happening in America. *The Monthly Heartlander.* Retrieved July 21, 2000, from http://www.heartlander

Berke, R. L. (2000, June 4). What are you afraid of? A hidden issue emerges. *New York Times.* Retrieved June 4, 2000, from http://www.nytimes.com/library/tech/00/04/biztech/articles/private-info-review.html

Bernstein, N. (1997a, September 15). High-tech sleuths find private facts online. *New York Times.* Retrieved September 22, 1997, from http://www.nytimes.com

Bernstein, N. (1997b, October 20). Proposals to protect privacy seem to face stalemate in contradictory goals. *New York Times*, A12.

Boruch, R. E., Cecil J. S. (Eds.). (1979). *Assuring the confidentiality of social research data*. Philadelphia: University of Pennsylvania Press.

Boruch, R. F. (1979). Methods for assuring personal integrity in social research: An introduction. In M. Bulmer (Ed.), *Censuses, surveys and privacy* (pp. 234–248). New York: Holmes & Meir Publishers.

Boruch, R. F., Cecil J. S. (Eds.). (1983). *Solutions to ethical and legal problems in social research*. New York: Academic Press.

Bunn, A. (2000, April 30). One or two things I'd rather you didn't know about me. *New York Times Magazine.* Retrieved May 3, 2000, from http://www.nytimes.com/library/magazine/home/200000430mag-austinbunn.html

Caruso, D. (1999, August 30). Consumers' desire for information privacy ignored. *New York Times.* Retrieved June 8, 2000, from http://www.nytimes.com/library/tech/99/08/biztech/articles/30digi.html

Census. (2000a, June 16). Proposed rule would delegate adjustment decision to census bureau director. *Census 2000 Initiative News Alert.* Available through census2000 listserv and at www.census2000.org

Census. (2000b, June 29). House fully funds remaining census 2000 operations, but some overseers concerned about rush to completion. *Census 2000 Initiative News Alert.* Available through census2000 listserv and at www.census2000.org

Census. (2000c, July 25). Census funding bill clears Senate committee. *Census 2000 Initiative News Alert.* Available through listserv Census2000@ccmc.org

Chandrasekaran, R. (1998, March 30). When the personal becomes public. *Washington Post National Weekly Edition*, pp. 10–12.

*Children's online privacy protection rule*, 64 Fed. Reg. 59888 (1999).

Clark, C. Z. F., & Coffey, J. L. (1984). How many people can keep a secret? Data interchange within a decentralized system. *Review of Public Data Use*, *12*, 271–277.

Clausing, J. (2000a, June 12). Gauging attitudes about the Internet. *New York Times.* Retrieved December 19, 2000, from http://www.nytimes.com/library/tech/00/06/biztech/articles/12mark.html

Clausing, J. (2000b, February 7). Report rings alarm bells about privacy on the Internet. *New York Times.* Retrieved February 7, 2000, from http://www.nytimes.com/library/tech/00/04/biztech/articles/07priv.htm

Clausing, J. (2000c, February 15). DoubleClick moves to quell privacy debate. *New York Times.* Retrieved May 10, 2000, from http://www.nytimes.com/library/tech/00/04/biztech/articles/0715priv.htm

Clausing, J. (2000d, February 11). Privacy lax at health Web sites. *New York Times.* Retrieved April 30, 2000, from http://www.nytimes.com/library/tech/00/02/cyber/articles/02privacy.html

Clausing, J. (2000e, April 18). New privacy law forcing changes to children's sites. *New York Times.* Retrieved April 30, 2000, from http://nytimes.com/library/tech/00/04/cyber/capital/18c.html

Clausing, J. (2000f, July 13). FTC finds no need for laws protecting online privacy. *New York Times.* Retrieved July 13, 1999, from http://www.nytimes.com/

CNET News.com. (2000, April 28). Intel to phase out processor serial numbers attacked by privacy advocates. *New York Times.* Retrieved May 3, 2000, from http://www.nytimes.com/library/tech/00/04/biztech/articles/29intel-privacy.html

Crano, L. F., Reagle, J., & Ackerman, M. S. (2000). *Beyond concern: Understanding net users' attitudes about online privacy* (AT&T Labs-Research Technical Report TR 99.4.3). Florham Park, NJ: AT&T Bell Labs-Research. Retrieved July 27, 2000, from http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm

David, M. H., & Robbin, A. (1989). *Database design for large-scale, complex data* (Survey of Income and Program Participation Working Paper 8923). Washington, DC: Bureau of the Census.

David, M. H., & Robbin, A. (1990). Computation using information systems for complex data. *Proceedings of the conference on advanced computing in the social sciences* (pp. 1–38). Oak Ridge, TN: Oak Ridge National Laboratory.

Dalenius, T. (1979). Data protection legislation in Sweden: a statistician's perspective. *Journal of the Royal Statistical Society*, *142*, 285–298.

Dalenius, T., Klevmarken A. (Eds.). (1976). *Personal integrity and the need for data in the social sciences*. Stockholm: Swedish Council for Social Science Research.

Duncan, G. T., Jabine T. B., de Wolf V. A. (Eds.). (1993). *Private lives and public policies*. Washington, DC: National Academy Press.

Duncan, J. W., Shelton W. C. (Eds.). (1978). *Revolution in United States government statistics, 1926–1976*. Washington, DC: Office of Federal Statistical Policy and Standards.

Durbin, J. (1979). Statistics and the report of the data protection committee [Great Britain]. *Journal of the Royal Statistical Society*, *142*, 299–306.

*Federal data banks and constitutional rights: A study of data systems on individuals maintained by agencies of the United States government* (Committee Print). Report prepared by the staff of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, U.S. Senate, 93rd Cong. (1974).

*Federal government statistics and statistical policy: hearing before a Subcommittee of the Committee on Government Operations, House of Representatives*, 97th Cong. (1982).

Fienberg, S. E., Martin M. E., Straf M. E. (Eds.). (1985). *Sharing research data*. Washington, DC: National Academy Press.

Fienberg, S. E., & Willenborg, L. C. R. J. (1998, December). Special issue on disclosure limitation methods for protecting the confidentiality of statistical data. *Journal of Official Statistics*, *14*(4), 337–565.

*Financial privacy: hearings before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Banking and Financial Services, House of Representatives*, 106th Cong. (1999).

Flaherty, D. H. (1978, August). Final report of the Bellagio conference on privacy, confidentiality, and the use of government microdata for research and statistical purposes. *Statistical Reporter*, *78*(8), 274–279.

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

Flaherty, D. H. (1989). *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: The University of North Carolina Press.

Frishberg, M. (2000, April 20). US confused about privacy. *Wired News.* Retrieved May 2, 2000, from http://www.wired.com/news/politics/0,1283,35979,00.html

*Genetics testing in the new millennium: advances, standards, and implications: Hearing before the Subcommittee on Technology of the Committee on Science, House of Representatives*, 106th Cong. (1999).

Glanz, J. (2000, July 16). Amid race profiling claims, Asian-Americans avoid labs. *New York Times*, pp. A1 and A12.

Gordon, A. C., Heinz J. P. (Eds.). (1979). *Access to information*. New Brunswick, NJ: Transaction Books.

Hammer, B. (2000, April 6). Census 2000 not connecting netizens. *Industry Standard: Intelligence for the Internet Economy.* Retrieved April 7, 2000, from http://thestandard.com/article/display/0,1151,13906,00.html

Harmon, A. (1997, September 22). On the office PC, bosses opt for all work, and no play. *New York Times*, pp. A1 and C15.

Hedrick, T. E., Boruch, R. F., & Ross, J. (1978). On ensuring the availability of evaluative data for secondary analysis. *Policy Sciences*, *9*, 259–280.

Hewitt, P. (1979). *Computers, records and the right to privacy.* Purley, Great Britain: Input Two-Nine.

Holmes, S. A. (2000a, March 17). Report says census bureau helped relocate Japanese. *New York Times*, p. A14.

Holmes, S. A. (2000b, August 30). Republicans keep pressing census bureau. *New York Times.* Retrieved December 27, 2000, from http://wwww.nytimes.com/2000/08/30/national/30CENS.html

Holmes, S. A. (2000c, September 30). Defying forecasts, census response ends declining trends. *New York Times.* Retrieved December 27, 2000, from http://www.nytimes.com/2000/09/20/national/20CENS.html

Holmes, S. A. (2000d, December 27). Census data is due as Congress braces for a reshuffling. *New York Times.* Retrieved December 27, 2000, from http://wwww.nytimes.com/2000/12/27/politics/27CENS.html

Hulett, D. T. (1977, July). Confidentiality of statistical and research data and the Privacy Act of 1974. *Statistical Reporter*, *75*(6), 197–209.

Hutchinson, A. (2000, March 3). Americans facing loss of personal privacy. *Congressional Record*, 106th Cong. Retrieved June 6, 2000, from http://thomas.loc.gov/

Jabine, T. B. (1975). The impact of new legislation on statistical and research uses of SSA data. *Proceedings of the American Statistical Association Social Statistics Section* (pp. 221–230). Washington, DC: American Statistical Association.

Johnston, D. C. (2000, January 3). New tools for the I.R.S. to sniff out tax cheats. *New York Times*, C1.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, *50*, 1193–1294. Retrieved May 6, 2000, from http://www.ntia.doc.gov/ntiahome/privacy/files/cprivacy.pdf

Kang, K. C. (2000, March 5). Asian-Americans can't shake "foreigner" label. *Milwaukee Journal Sentinel*, p. 8A.

Keizer, G. (1997, October). Private parts: Your private life isn't so private on the Web. *Computerlife*, pp. 52, 54, 56.

Kim, J. J., & Winkler, W. E. (1997). *Masking microdata files (Research Report 9703)*. Washington, DC: Bureau of the Census. Retrieved June 7, 2000, from http://www.census.gov/srd/papers/pdf/rr97-3.pdf

Kingston, J. (2000, March 16). Census Bureau should consult Reader's Digest. *Congressional Record*, 106th Cong. Retrieved June 6, 2000, from http://thomas.loc.gov

Koppell, J. G. S. (2000, June 19). On the Internet, there's no place to hide. *Industry Standard*, *4*(23). Retrieved June 19, 2000, from http://www.thestandard.com/article/display/0,1151,155850,00.html

Lewis, P. H. (2000, February 10). Losing privacy in the age of the Internet [Review of the book *Database Nation: The Death of Privacy in the 21st Century*]. *New York Times.* Retrieved May 3, 2000, from http://www.nytimes.com/library/tech/00/02/circuits/articles/10revu.html

Lohr, S. (1997, March 17). Feeling insecure, are we? *New York Times*, pp. C1, C7.

Lott, T. (2000, April). *Census 2000 is Mississippi's future* (press release). Retrieved July 20, 2000, from http://lott.senate.gov/news/2000/0406.census.html

Louis Harris and Associates. (1984). *The road after 1984*. New York: Louis Harris and Associates.

Louis Harris and Associates, & Westin, A. F. (1979). *The dimensions of privacy: A national opinion research survey of attitudes toward privacy.* Stevens Point, WI: Sentry Insurance.

Lyons, G. M. (1969). *The uneasy partnership: Social science and the federal government in the twentieth century.* New York: Russell Sage Foundation.

Markoff, J. (1998, July 1). Differences over privacy on the Internet. *New York Times*, pp. C1 and C7.

Markoff, J. (2000, May 6). Law officials seek origins of the virus. *New York Times.* Retrieved May 6, 2000, from http://www.nytimes.com/library/tech/00/05biztech/articles/06virus.html

Marsan, C. D. (2000, November 30). Online privacy law anticipated. *InfoWorld.com.* Retrieved December 1, 2000, from http://www2.infoworld.com

Martin, E. (2000, May). *Changes in the public's privacy concerns during the census: Comparisons with 1990*. Paper presented at the annual meeting of the American Association of Public Opinion Research, Portland, OR.

Martin, M. E., & Straf, M. L. (1992). *Principles and practices for a federal statistical agency.* Washington, DC: National Academy Press.

McAdams, R., Smelser N. J., Treiman D. J. (Eds.). (1982). *Behavioral and social science research: A national resource (Part I)*. Washington, DC: National Academy Press.

McCullagh, D., & Morehead, N. (2000, July 20). FTC goes public with privacy. *Wired News.* Retrieved July 25, 2000, from http://www.wired.com/news/print/0,1294,37695,00.html

McGuire, D. (2000a, November 30). Americans cautiously willing to share info online — study. *newsbyte.com.* Retrieved November 30, 2000, from http://www.newsbytes.com/news/00/158801.html

McGuire, D. (2000b, December 2). Net privacy law could pass, despite congressional rancor. *Newsbytes.com.* Retrieved December 5, 2000, from http://www.newsbytes.com/news/00/159002.html

McGuire, D. (2000c, December 8). Key committee faces choices on broadband, privacy. *Computer*. Retrieved December 20, 2000, from http://222.computeruser.com/news/00/12/08/news8.html

*Medical information protection and research enhancement act of 1999: Hearing before the Subcommittee on Health and Environment of the Committee on Commerce, House of Representatives*, 106th Cong. (1999).

*Medical records confidentiality in a changing health care environment: Hearing of the Committee on Health, Education, Labor, and Pensions, Senate*, 106th Cong. (1999).

*Medical records confidentiality in the modern delivery of health care: Hearing before the Subcommittee on Health and Environment of the Committee on Commerce, House of Representatives*, 106th Cong. (1999).

*Medical records privacy: Hearing in Berlin, VT of the Committee on Health, Education, Labor, and Pensions, Senate*, 106th Cong. (1999).

Mochmann, E., & Müller, P. M. (1979). Data protection and access to social-science data. *International Social Science Journal*, *31*(1), 162–165.

Mochmann, E., Müller P. M. (Eds.). (1979). *Data protection and social science research: Perspectives from ten countries*. Frankfurt: Campus Verlag.

Monk, L. R. (2000, October 23). My data, mine to keep private. *New York Times.* Retrieved November 27, 2000, from http://www.nytimes.com/2000/10/23/opinion/23MONK.html

Mosquiera, M. (2000a, June 15). Lawmakers seek balance in privacy legislation. *New York Times.* Retrieved June 15, 2000, from http://www.ntimes.com/library/. . ./TWB20000615S0017.html

Mosquiera, M. (2000b, December 7). Ranks of privacy "pragmatists" are growing. *TechWeb.* Retrieved December 20, 2000, from http://www.techweb.com/wire/story/TWEB2000/1207S0002

Myers, S. (2000, February 26). Census Bureau begins count with 120 million wrong addresses. *New York Times.* Retrieved June 22, 2000, from www.nytimes.com/library/national/022600census-count.html

National Opinion Research Center. (1996). Codebook variable: Databank. *General social survey*. Chicago: National Opinion Research Center. Retrieved July 27, 2000, from http://www.icpsr.umich.edu/GSS99/codebook/databank.htm

Naylor, J., & Upton, J. (1999, February 12). Medical industry lax on Internet security. *Detroit News.* Retrieved April 27, 2000, from http://detroitnews.com/1999/metro/9902/12/02120124.htm

Nie, N. H., & Junn, J. (2000, May 4). *America's experience with Census 2000: A preliminary report*. Retrieved May 24, 2000, from http://www.intersurvey.cm/about_intersurvey/press/05042000_census.html

Nie, N. H., Junn, J., & Slotwiner, D. (2000, May). *The 2000 Census civic mobilization effort: Influences on participation*. Paper presented at the annual meeting of the American Association of Public Opinion Research, Portland, OR.

Norman, J. (2000a, March 25). Census training materials had historical errors, bureau admits. *Milwaukee Journal Sentinel*, p. 1B.

Norman, J. (2000b, March 27). From pep rallies to pet peeves, census 2000 gets most hype, flap. *Milwaukee Journal Sentinel*, p. 1B.

O'Harrow Jr., R. (1998, March 23). Say goodbye to privacy. *Washington Post National Weekly Edition*, pp. 12–14.

O'Harrow Jr., R. (2000, December 5). Internet firms act to ease sharing of personal data. *Washington Post*, p. E01. Retrieved December 20, 2000, from http://washingtonpost.com/wp-dyn/articles/A23676-2000Dec4.html

Okie, S. (2000, April 16). Groups warn of breaches in privacy laws for patients. *Washington Post*, p. A02.

Olse, S. (2000, November 8). Geographic tracking raises opportunities, fears. *CNETNews.com.* Retrieved November 20, 2000, from http://news.cnet.com/news/0-1005-200-3424168.html

Omega World Travel (2000, February 10). *Hackers hit Omega Travel (press release)*. Retrieved February 10, 2000, from http://www.biz.yahoo.com/prnews/00210/va_omega_t_l.html

*Oversight of computer matching to detect fraud and mismanagement in government programs: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Senate*, 97th Cong. (1982).

*Oversight of the Privacy Act of 1974: Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives*, 98th Cong. (1983).

Pear, R. (2000a, December 20). Clinton will issue new privacy rules to shield patients. *New York Times.* Retrieved December 20, 2000, from http://www.nytimes.com/2000/12/20/national/20PRIV.html

Pear, R. (2000b, December 21). New privacy rules are challenged. *New York Times.* Retrieved December 21, 2000, from http://www.nytimes.com/2000/12/21/national/21PRIV.html

Peterson, I. (1997, July 14). Public information, business rates. *New York Times*, pp. C1 and C8.

Pew Research Center for the People and the Press. (1999). *Public perspectives on the American century: technology triumphs, morality falters*. Washington, DC: Pew Research Center for the People and the Press. Retrieved on July 19, 2000, from http://www.people-press.org/mill1rpt.htm

Pew Research Center for the People and the Press. (2000). *Performance and purpose: constituents rate government agencies*. Washington, DC: Pew Research Center for the People and the Press. Retrieved July 19, 2000, from http://www.people-press.org/npr00rpt.htm

Pitofsky, R. (2000, May 25). *Prepared statement of the Federal Trade Commission on "Privacy online: fair information practices in the electronic marketplace," before the Committee on Commerce, Science, and Transportation, U.S. Senate*. Washington, DC: Federal Trade Commission. Retrieved December 27, 2000, from http://www.ftc.gov/2000/05/testimony/privacy.htm

Pritchard, T. (2000, December 23). Canada strengthens Internet privacy. *New York Times.* Retrieved December 23, 2000, from http://www.nytimes.com/2000/12/23/technology/23PRIV.html

Privacy Foundation. (2001). *Workplace surveillance is the top privacy story of 2000*. Retrieved January 3, 2001, from http://www.privacyfoundation.org/release/top10.html

Privacy Protection Study Commission. (1977). *Personal privacy in an information society.* Washington, DC: U.S. Government Printing Office.

*Privacy of medical records: Hearings before a Subcommittee of the Committee on Government Operations on H.R. 2979 and H.R. 3444, House of Representatives*, 95th Cong. (1979).

*Privacy under a microscope: Balancing the needs on research and confidentiality: hearing of the Committee on Health, Education, Labor, and Pensions, Senate*, 106th Cong. (1999).

*Public reaction to privacy issues: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives*, 96th Cong. (1979).

Richtel, M. (2000, March 31). Yahoo says it is discussing Internet privacy with the F.T.C. *New York Times*, p. C5.

Riecken, H. W., & Boruch, R. F. (1978). Social experiments. *American Review of Sociology*, *4*, 511–532.

Robbin, A. (1981). *The social utility of personal information*. Madison, WI: State Historical Society of Wisconsin.

Robbin, A. (1984). *A phenomenology of decision making: Implementing information policy in state health and welfare agencies*. Unpublished doctoral dissertation, University of Wisconsin-Madison.

Robbin, A. (1995). SIPP ACCESS, an information system for complex data: A case study in creating a collaboratory for the social sciences. *Internet Research: Electronic Networking Applications and Policy*, *5*(2), 37–66.

Robbin, A., & David, M. H. (1988). SIPP ACCESS: Information tools improve access to national longitudinal panel surveys. *Research Quarterly*, *27*, 499–515.

Robbin, A., & Jozefacki, L. (1982). *Public policy on health and welfare information: Compendium of state legislation on privacy and access*. Madison, WI: University of Wisconsin, Data and Program Library Service.

Robbin, A., & Koball, H. (2001, October). Seeking explanation in theory: Reflections on the social practices of organizations that distribute public use microdata files for research purposes. *Journal of the American Society for Information Science and Technology, 52*(13), 1169–1189.

Rodger, W. (2000, November 27). Bucking privacy. *Interactive Week.* Retrieved December 20, 2000, from http://www.zdnet.com/intweek/stories/news/0,4164,2659139,00.html

Rosenbaum, D.E. (2000, April 1). Seeking answers, census is stirring privacy questions. *New York Times.* Retrieved June 6, 2000, from http://www.nytimes.com/library/national/040100privacy-census.html

Roth, S. (1981, February 15). Census bureau aided '42 roundup of Nisei. *Washington Post*, p. G2.

Rubin, E.J. (2000, February 2). California and the West: some health care Web sites lack privacy. *Los Angeles Times.* Retrieved May 6, 2000, from Lexis-Nexis database. Available at: http://web.lexis-nexis. com/universe

Ruggles, S. (2000a, June 2). *PUMS 2000 news*. Listserv keep_informed@hist.umn.edu

Ruggles, S. (2000b, November 6). *News on 2000 PUMS*. Listserv keep_informed@pop.umn.edu

Sanders, E. (2000, December 11). Web privacy programs are scrutinized. *LaTimes.com.* Retrieved December 20, 2000, from http://www.latimes.com

Sasfy, J. H., & Siegel, L. G. (1981a). *A study of research access to confidential criminal justice agency data*. McLean, VA: The MITRE Corporation.

Sasfy, J. H., & Siegel, L. G. (1981b). *The impact of privacy and confidentiality laws on research and statistical activity*. McLean, VA: The MITRE Corporation.

Savage, M., & Stirpe, A. (2000, December 1). Under surveillance. *CRN.* Retrieved December 20, 2000, from http://www.crn.com/Comp. . .s/Search/Article.asp?Article!D=22049

Schneier, B. (1999, June 15). Risks of e-mail borne viruses, worms, and Trojan Horses. *RISKS-List: Risks-Forum Digest*, *20* (45). Retrieved June 17, 1999, from http://catless.ncl.ac.uk/Risks/20.45.html@subj2

Seltzer, W., & Anderson, M. (2000, March). *After Pearl Harbor: The proper role of population data systems in time of war*. Paper presented at the annual meeting of the Population Association of America, Los Angeles, CA.

Seminario, M. (1998, May 23). *Lesson of hacker incident: Credit card numbers not necessarily safe online—yet*. Retrieved July 15, 1998, from http://www5.zdnet.com/zdnn/content/zdnn/0523/zdnn0010.html

Sieghart, P. (1976). *Privacy and computers*. London: Latimer New Dimensions.

Singer, E. (1978). Informed consent: Consequences for response rates and response quality in social surveys. *American Sociological Review*, *43*, 144–163.

Singer, E. (1983). Informed consent procedures in surveys: Some reasons for minimal effects on response. In R. F. Boruch, & J. S. Cecil (Eds.), *Solutions to ethical and legal problems in social research* (pp. 183–211). New York: Academic Press.

Singer, E., Mathiowetz, N. A., & Couper, M. P. (1993, Winter). The impact of privacy and confidentiality concerns on survey participation: The case of the 1990 U.S. census. *Public Opinion Quarterly*, *57*(4), 465–482.

Skerry, P. (2000). *Counting on the census? Race, group identity, and the evasion of politics*. Washington, DC: Brookings Institution Press.

Smith, N. (2000, March 28). Many census questions too intrusive. *Congressional Record*, 106th Cong.

Smith, T. W. (1990, December). *Security awareness and the climate of public opinion*. Paper presented to the symposium on security awareness: the challenge of the 1990s, Monterey, CA. Paper available from the author and abstract available at http://www.icpsr.umic.edu/GSS99/bib/02997.htm

Spruill, N. L. (1984). The confidentiality and analytic usefulness of masked business microdata. *Review of Public Data Use*, *12*, 307–314.

*Standards for Privacy of Individually Identifiable Health Information*. Final Rule, 65 Fed. Reg., 82461 (2000) (to be codified at 45 C. F. R §160, 164).

Stellin, S. (2000, December 4). Dot-com liquidations put consumer data in limbo. *New York Times.* Retrieved December 4, 2000, from http://www.nytimes.com/2000/12/04/technology/02NET.html

*The computer and invasion of privacy: Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives*, 89th Cong. (1966).

The European Commission. (1997). *Data protection: Annual report of the Data Protection Working Party.* Retrieved November 7, 2000, from http://europa.eu.int/comm/internal_market?media/dataprot/wpdocs/wp3en.htm

The Industry Standard. TRUSTe to launch EU Safe Harbor seal. (2000, November 1). *TheStandard.com.* Retrieved November 7, 2000, from http://thestandard.com/article/article_print/0,1153,19846,00.html

Traficant, J. A. (2000, March 28). Census Bureau out of control. *Congressional Record,* 106th Cong. Retrieved June 6, 2000, from http://thomas.loc.gov

Treese, W. (2000, December). Data collection and consumer privacy. *netWorker*, *4*(4), p. 9.

University of California at Los Angeles Center for Communication Policy. (2000, October). The UCLA Internet report: surveying the digital future. Los Angeles: University of California at Los Angeles Center for Communication Policy. Retrieved November 20, 2000, from http://www.ccp.ucla.edu

University of California at Los Angeles. Law Review Research Project. (1968). Computerization of government files: What impact on the individual? *UCLA Law Review*, *15*(5), 1371–1498.

University of Minnesota Population Center and the Inter-University Consortium for Political and Social Research. Census 2000 Advisory Committee. (2000, May 22). *The public use microdata samples of the U.S. census: Research applications and privacy issues*. Report prepared for Census 2000 Users' Conference on PUMS, Alexandria, VA. Retrieved July 23, 2000, from http://www.ipums.umn.edu/~census2000/

Upton, J. (1999, February 12). U-M medical records end up on Web. *Detroit News.* Retrieved April 27, 2000, from http://detroitnews.com/1999/metro/9902/12/02120114.htm

U.S. Bureau of the Census. (1964). *Census of population and housing. 1960 public use sample: One-in-one-thousand sample*. Washington, DC: Government Printing Office.

U.S. Bureau of the Census. (1972). *Public use microdata samples of basic records from the 1970 census: Description and technical documentation*. Washington, DC: Government Printing Office.

U.S. Bureau of the Census. (1973). *Technical documentation for the 1960 public use microdata sample*. Washington, DC: Government Printing Office.

U.S. Bureau of the Census. (1984). *Census of population, 1940: Public use microdata sample technical documentation*. Washington, DC: Government Printing Office.

U.S. Bureau of the Census. (1993a). Appendix C. Accuracy of the data. *STF3 technical documentation*. Washington, DC: U.S. Bureau of the Census. Retrieved July 23, 2000, from http://www.census.gov/td/stf3/append_c.html

U.S. Bureau of the Census. (1993b). Appendix B. Definitions of subject characteristics. *STF3 technical documentation*. Washington, DC: U.S. Bureau of the Census. Retrieved July 23, 2000, from http://www.census.gov/td/stf3/append_b.html#INCOME

U.S. Bureau of the Census. (2000, October 19). *The U.S. Census Bureau's recommendations concerning the census 2000 public use microdata sample (PUMS) files*. Washington, DC: U.S. Bureau of the Census.

U.S. Department of Commerce. (1999, November 8). *U.S. Secretary of Commerce William M. Daley calls for consumer privacy protection in online profiling* (news release). Retrieved June 6, 2000, from www.doc.gov/20release.html

U.S. Department of Commerce. (2000). *Welcome to the Safe Harbor*. Retrieved December 29, 2000, from http://www.export.gov/safeharbor.

U.S. Department of Health, Education and Welfare. (1973). *Records, computers, and the rights of citizens: A Report of the Secretary's Advisory Committee on Automated Personal Data Systems (DHEW Publication No. (OS) 73-94)*. Washington, DC: Government Printing Office.

U.S. Federal Committee on Statistical Methodology. (1994). *Report on statistical disclosure limitation methodology (Statistical Policy Working Papers 22)*. Washington, DC: Department of Commerce.

U.S. Federal Committee on Statistical Methodology. (1999, July). *Checklist on disclosure potential of proposed data releases*. Washington, DC: Office of Management and Budget.

U.S. Federal Trade Commission. (1998, June). *Privacy online: A report to Congress*. Washington, DC: U.S. Federal Trade Commission. Retrieved April 24, 2000, from http://www.ftc.gov/reports/privacy/toc.htm

U.S. Federal Trade Commission. (2000, May). *Privacy online: Fair information practices in the electronic marketplace: a report to Congress*. Washington, DC: U.S. Federal Trade Commission. Retrieved December 27, 2000, from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

U.S. Internal Revenue Service. Statistics of Income Division. (1985, December). *Record linkage techniques—1985*. Washington, DC: Department of Treasury.

U.S. National Research Council. Committee on Federal Agency Evaluation Research. (1975). *Protecting individual privacy in evaluation research*. Washington, DC: National Academy of Sciences.

U.S. National Research Council, Committee on National Statistics. (1979). *Privacy and confidentiality as factors in survey research*. Washington, DC: National Academy Press.

U.S. National Research Council, Committee on National Statistics. (2000). *Improving access to confidentiality of research data: Report of a workshop*. Washington, DC: National Academy Press.

U.S. National Science Board, Special Commission on the Social Sciences. (1969). *Knowledge into action: Improving the nation's use of the social sciences*. Washington, DC: National Science Foundation.

U.S. National Technical Information Administration (2000). Closing the digital divide. Retrieved October 18, 2000, from http://www.digitaldivide.gov/

U.S. Office of Federal Statistical Policy and Standards. (1978a). *A framework for planning U.S. federal statistics in the 1980's*. Washington, DC: Department of Commerce.

U.S. Office of Federal Statistical Policy and Standards. (1978b). *Report on statistical disclosure and disclosure avoidance techniques* (Statistical Policy Working Paper 2). Washington, DC: Department of Commerce.

U.S. Office of the President. (2000, December 20). *President Clinton issues strong new consumer protections to ensure the privacy of medical records*. Retrieved December 28, 2000, from www.whitehouse.gov/WH/new/html/Wed_Dec_20_141343_2000.html

U.S. Privacy Protection Study Commission. (1977). *Personal privacy in an information society*. Washington, DC: Government Printing Office.

U.S. Social Security Administration. (1973). *Studies from interagency data linkages*. Washington, DC: U.S. Social Security Administration.

Weingart, P. (1982). The social assessment of science, or the de-institutionalization of the scientific profession. *Science, Technology, and Human Values*, *7*, 53–55.

Weinstein, L. (1997, January 17). Your signature for sale? *PRIVACY Forum Special Report*. Retrieved February 15, 2000, from http://www.vortex.com

Weinstein, L. (1999, November 1). "Spies" in your software? *PRIVACY Forum Special Report*. Retrieved May 10, 2000, from http://www.vortex.com

Weinstein, L. (2000, April 20). Massive tracking of Web users planned — via ISPS. *Internet Privacy Forum*, *9*(13). Retrieved April 20, 2000, from http://vortex.com/privacy/priv.09.13

Weiss, C. H. (1977a). Research for policy's sake: the enlightenment function of social research. *Policy Analysis*, *3*(4), 531–545.

Weiss, C. H. (1977b). *Using social research in public policy making*. Lexington, MA: Lexington Books.

Westin, A. F. (Ed.). (1971). *Information technology in a democracy*. Cambridge, MA: Harvard University Press.

Westin, A. F. (1976a). *Computers, health records, and citizens rights*. Washington, DC: Government Printing Office.

Westin, A. F. (1976b). *Privacy and freedom*. New York: Atheneum.

Westin, A. F., & Baker, M. A. (1972). *Databanks in a free society: Computers, record-keeping and privacy*. New York: Quadrangle/The New York Times Book Co.

Wilson, O. H., & Smith, W. J. (1984). Access to tax records for statistical purposes. *Review of Public Data Use*, *12*, 295–306.

Winkler, W. E. (1997). *Views on the production and use of confidential microdata* (Research Report #9701). Washington, DC: Bureau of the Census. Retrieved June 7, 2000, from http://www.census.gov/srdpapers/pdf/rr97-1.pdf.

Winkler, W. E. (1998). *Producing public use microdata that are analytically valid and confidential* (Research Report #9802). Washington, DC: Bureau of the Census. Retrieved June 7, 2000, from http://www.census.gov/srd/papers/pdf/rr9802.pdf

Winkler, W. E. (1999). *The state of record linkage and current research problems* (Research Reports #99-01). Washington, DC: Bureau of the Census. Retrieved April 28, 2000, from http://www.census.gov/srd/papers/pdf/rr99-01.pdf

Wulff, K. M. (Ed.). (1979). *Regulation of scientific inquiry: Societal concerns with research* (American Association for the Advancement of Science Selected Symposium 37). Boulder, CO: Westview Press.

**Alice Robbin** is Associate Professor of library and information science in the School of Library and Information Science at Indiana University at Bloomington. Her research interests include information policy, communication and information behavior in complex organizations, and the societal implications of the digital age. In addition to her research on the consequences of privacy law and policy for social research, she is currently examining the political controversy over the federal reclassification of standards for racial and ethnic group data.