# Data Confidentiality, Social Research and the Government

DAVID F. LINOWES
MICHELE M. HOYMAN

THIS PAPER ADDRESSES the issue of confidentiality and privacy of information contained in archives and libraries. To do so in a meaningful way requires an analysis of the broad issue of information privacy in general prior to examining its relationship to the functions of the librarian and archivist.

There is no generally accepted definition of privacy. No less a figure than Supreme Court Justice Louis Brandeis spoke, in 1890, of the individual's "right to be let alone" as being the most valued right of civilized man.[1] Twenty years before that, a Michigan judge ruled that privacy was a "constitutional" right. In fact, privacy rights are not specifically spelled out in the Constitution, although the implication is clearly there. The Third Amendment prohibits the lodging of soldiers in private homes without the owner's consent. The Fourth Amendment protects citizens against arbitrary government search. Furthermore, courts have been interpreting a right to privacy from the Fifth Amendment, which protects against self-incrimination; the First Amendment, which guarantees freedom of speech and assembly; and the Ninth Amendment, which reserves to the people all rights not specifically delegated to the states and federal government.

The Privacy Act of 1974, which established the Privacy Commission[2] and placed certain constraints on federal agencies, for the first time

David F. Linowes is Professor of Political Economy and Public Policy, School of Social Sciences, and Michele M. Hoyman is Assistant Professor, Institute of Labor and Industrial Relations, University of Illinois at Urbana-Champaign.

gave statutory recognition to a right of privacy, but did not define it. The present, rather urgent concern for this undefined right results from two phenomena in America that are having revolutionary impacts on society: the rapid advances of computer technology and the ever-increasing expections which the individual has of both government and business. Technological developments have been so drastic that it is difficult for persons of our generation to comprehend them. We now have the technology to store 100 million pieces of information on an inch-square silicon chip. And the cost of this storage on a piece of silicon has been declining at such amazing rates that it is sometimes argued it is cheaper to store data than to destroy them. The power of silicon has proven remarkable in its ability literally to transform society.

The computer was developed in the 1940s. Early models contained large, bulky vacuum tubes, so that a 1950s computer filled an entire room. With the invention of the transistor, computers grew smaller, but the next generation witnessed a quantum leap forward with the introduction of the silicon chip. Now the inch-square "miracle chip" has the calculating capabilities of an entire roomful of computer hardware of the 1950s. A million-dollar computing capacity of three decades ago costs twenty dollars today, and is 100,000 times faster.[3] Work that required one day then is now done in less than one minute. Data contained in a computer data bank are being transmitted across nations and oceans by way of satellite with the speed of light.

Throughout history, societies have had to adjust when great technological breakthroughs have occurred. It happened with the invention of the printing press, the steam engine, the electric light, the automobile. One of the major convulsions in this generation is being triggered by computer technology. Unfortunately, the law and organizational practices have been lagging behind technological developments. The irony of technology may be that it enables society to gain control over everything, except technology.

The other phenomenon, that of individuals demanding an increasing number of services from all institutions, continues to grow at what appears to be a never-ending pace. From the government the public expects social security, unemployment compensation, guaranteed mortgage loans, and all levels of welfare. From business, the public expects credit cards which give instant credit approval any place in the world, and the ability to make plane reservations in a matter of minutes for any kind of trip to anywhere. Libraries themselves are being called upon to render more and more personal and community services. There is a trend toward computerization to provide faster user service within a

library, and there is a trend toward networks to provide services across libraries.

Administrators responsible for furnishing these services must satisfy themselves of an individual applicant's eligibility by demanding and getting more personal, often sensitive, information. Thus, more and more confidential data are being injected into the system of government and business, never to be destroyed.

Today, data have become, in effect, a new element. They are almost never destroyed, and any one item can be retrieved in seconds. During the manual era, data were regularly destroyed, largely because of the cost of storage. Manual retrieval of one record out of a million was costly and time-consuming, often requiring months. Therefore, masses of accumulated personal data had very limited utility.

## Threats to Privacy

The continuation of these developments means that certain practices have developed which are threats to privacy. The following are some of those which a federal policy of privacy protection should address.

*List Compilers*

Among the organizations that thrive in this country are some that monitor the activities of individuals and report thereon to their subscribers for a fee. For example, there is an organization outside of Chicago that professes to identify those persons in this country who are known to be "attacking or ridiculing a major doctrine of the Christian faith or the American way of life." These include authors of books and articles, speakers, and even signers of group advertisements in leading newspapers. In this organization's files are even the names of those individuals who had been involved with the long-defunct House Un-American Activities Committee. If a person's name appears in its file, he or she is characterized as a person with anti-American or anti-Christian attitudes, and investigative companies using its service so report to their clients.

These lists are developed by obtaining names and addresses from public records such as census tract data and automobile registrations, and by renting lists from private industry, such as magazine and book publishers, credit card companies, and charitable organizations. They are then combined into various configurations by computer to develop desired profile groupings. The final profiled lists are rented out for about three and one-half cents a name.[4]

The inclusion of the name and address of a person on one of those profile listings is the basis for an individual being so characterized, whether justified or not. This information in a person's file could be a contributing factor for an adverse decision, be it an important appointment, promotion or granting of credit. The point is that the affected individual does not know that this information is the basis of an adverse decision nor that this information is being kept. A federal privacy policy, following the general principles established by the Privacy Commission, provides for the right of access of an individual to his or her records and the right to "correct" these records if they are inaccurate. A privacy policy would also limit the right of certain holders of information, such as employers, to violate the confidentiality of employees by providing third parties, such as the list compilers, with such information without the employee's knowledge or consent.

*Financial Records*

Most people regard their finances as a strictly personal and somewhat sensitive matter. They believe, perhaps innocently, that a financial dealing is a confidential matter between them and their banks, creditors or credit card companies. Unfortunately, most people have little concept how seriously their expectation of confidentiality has been compromised.

Checking account and credit card records for the average person constitute, in effect, an economic and social diary, and yet they are increasingly exposed to a wide array of other persons, such as employers, landlords and just curious neighbors. The recently passed Financial Right of Privacy Act of 1978 places limited constraints on some government agencies' access to financial records, but in most areas the government has almost unbridled access to such records. For private sector inquirers, there are few limitations.

*Medical Records and Insurance*

Everyone is the subject of medical files, usually more than one. Yet, many people are not aware of how available this information is to insurance companies, employers or anyone else who might have an interest in an individual's medical history for virtually any purpose.

Denver District Attorney Dale Tooley found that private medical records can be and have been improperly obtained from most hospitals in the Denver area, not to mention a "remarkable number of clinics and doctors' offices." He tells of people posing as doctors, nurses and even clerics to get medical records which they can sell. Some insurance companies, employers and others are a market for this information.

Organizations that use such services may know more about a person's medical condition than the individual, since medical practitioners do not generally allow a patient to see his or her own records. Laws are inadequate to protect against this kind of behavior, which apparently is sponsored throughout the country by some of the largest companies. The need for more protection of the individual in this area is obvious. The Medical Records Act, which is currently in Congress, provides for guarantees of the privacy of an individual's medical records by forbidding their disclosure without the employee's written permission.

**Broader Implications of Privacy**

In general, it is widely believed that the balance of power in our society is becoming more and more dangerously weighted in favor of large institutions—government and industry alike. A chief reason is that they are the ones with the information.

In the political arena, computerized capabilities have given pressure groups the power to influence candidate selection and key legislative issues in ways not available before. Massive direct-mail campaigns are key weapons in a lobbyist's arsenal. Information regarding the likes and dislikes, political leanings and preferences of specific groups of Americans is so comprehensive that in some cases an election can be determined before the voting begins. Confirmation by fast information retrieval and the importance of the media in reporting this information are together fundamentally altering the nature of the political process in ways which we are just begining to know.

Furthermore, this is not a problem which is confined to the United States; in fact, the technological problem itself may create problems for the relations between countries. For instance, some nations want to create electronic barriers to halt the flow of information. They consider information within a country a national resource, much like copper or oil. If information does cross their borders electronically, they want to charge a tariff on it.

The lack of controls over information transmission for processing or use in another country leaves developed nations concerned and developing nations alarmed. Economic data, government data, data from home offices of multinational corporations are beamed through the sky in the normal course of business today. Technology in the United States has advanced so far that many developed countries, as well as Third World countries, lag behind. For example, much information is coming into the United States from Canada for processing, classifying and analyzing because it can be handled much more effectively and

economically here. It is just as cheap to beam data across a border or an ocean as it is to beam it next door. Hundreds of millions of dollars of foreign exchange are exported from Canada to the United States to pay for this service. By 1985, it is estimated that it will cost Canada $1.5 billion per year in foreign exchange, and Canada will lose 25,000 jobs.[5] Several nations have established government agencies to administer privacy and trans-border data laws. The impact of this development on librarians and archivists will be most far-reaching.

## Role of Libraries in an Information Society

The general image of the librarian's role is one of guardian of circulation records as well as researcher of reference questions for library users. As such, the library has access to certain information about users which may be considered confidential. In the circulation and reference capacity, there is a simple direct link between the user whose confidentiality needs to be protected and the professional who is the protector of this confidentiality. However, the increasing computerization of both circulation and reference systems means that access to these records has increased.

Librarians also may have other roles than just in a circulation or reference capacity. The librarian may be an archivist, in which case the professional's role becomes more complicated. The role of the archivist differs substantially from that of the librarian as regards confidentiality. The job of the librarian is to make available all materials to the user, guaranteeing the nature of the user's research question and the particular sources used as confidential. The role of the archivist differs significantly from that of librarian in that he or she exerts control over who can use the collection, and must protect the "implicit trust" of the deposit of the records by assuring that only serious scholars use the collection.[6] For instance, the librarian would not think of querying the user as to why he or she was interested in a certain topic. However, an archivist will not only question potential users, but will make a professional judgment as to which person will be permitted access to the collection. Therefore, the librarian is concerned solely with defending the intellectual freedom of the reader and his/her right to privacy, whereas the archivist plays a gatekeeper role, sometimes blocking the researcher's access if the researcher is not considered a "serious" scholar. Moreover, the librarian will not necessarily release information on who is researching a certain topic, yet the historical archivist will as a matter of courtesy and ethics indicate to a serious researcher the names of other researchers who have used the collection.

Another role of the librarian as computerization increases is as data archivist for large social science data collections. At the moment this may not be a primary concern of the profession, but as an increasing number of centralized information systems are established, the skills that librarians have will be needed—skills such as cataloging, retrieval and reference. Secondly, the more these resources are developed, the more libraries may be called upon to include in their catalog and reference service a list of social science data sources available. Thus, a librarian can function in two capacities: directly as an archivist who catalogs the vast amount of information in a data set, or as a reference librarian who can help the user find the appropriate codebook and study in order to research a topic. The goal of an archivist is to maximize the use of the data, but the increased use will pose an increased risk of violating confidentiality. Therefore, the role of an archivist in protecting privacy becomes critical.[8]

A final role of libraries which should be mentioned is their role as employers. As employers, they face the same issues regarding the privacy of personnel records as private sector employers. The suggestion here is that library personnel practices, like the practices of many private sector employees, may violate the employee's right to privacy. This may be because of the lack of confidentiality of personnel records, or because of other employment practices which violate employee privacy.

**Public Visibility of Information Privacy Problems for Libraries**

More specific and more visible aspects of information privacy problems involving libraries and archives usually come to the attention of the public through a controversial incident, such as when a librarian refuses to reveal to a law enforcement agency the name of a person who checked out a certain book. Some of the incidents concerning the confidentiality of circulation records became quite controversial, attracting the attention of an entire community.

In 1970, in both Milwaukee and Atlanta, U.S. Treasury agents requested all slips and inquiries for books on explosives. In Milwaukee, the city attorney ruled that such records were "public records," at which point the librarian complied. In the Atlanta Public Library, the same request was denied in the absence of a subpoena.[9]

In another case, the Seattle Public Library in 1974 released its 1970 circulation records to the FBI when the agency presented a subpoena for the records in connection with a forgery case.[10] In 1974 in Los Alamos, Texas, FBI agents requested the librarian to release the circulation records of certain individuals included on a "subversive" list. The

library refused and said that a court order would be required.[11]

In 1979 when a police officer in Sudbury, Massachusetts, found a bag of marijuana hidden in the *Oxford Book of American Verse* and asked who had checked the book out, the library director, Helen Lowenthal, refused to tell him.[12] Lowenthal cited the code of ethics that librarians have regarding the confidentiality of the user-librarian relationship. The library's board of trustees subsequently adopted the ALA policy passed in 1971 regarding confidentiality.[13]

In many cases the reason for the controversy is not the release of circulation records, but the disclosure of a person's reference question—information which librarians consider confidential under their code of ethics. In 1979 in Connecticut, police investigating the burning of a cross asked the library for names of persons using materials on the Ku Klux Klan.[14] In 1979, state criminal investigators in Iowa asked the Des Moines Public Library to provide names of borrowers of books on occult practices. The officers were investigating cattle mutilations thought to be the result of cult rites.[15] In 1980, in Texas, police officers asked a public library to provide the names of all persons who had borrowed chemistry manuals found at the site of an illegal drug lab.[16]

Not infrequently, privacy problems stem from private citizens who want to spy on one another, and have nothing to do with law enforcement. For example, in 1978 a Kansas newspaper editor demanded access to library circulation records as records open to the public. He wanted to know whether city council members who had rejected a new library building used library services.[17] A divorced father in Illinois wanted access to a library's story-hour records to make certain his child was using his name and not that of the mother's second husband.[18] In 1977 a newspaper editor in Washington State demanded access to the records of a community college library in order to prove that tax dollars were wasted on projectors and other equipment available for loan.[19]

## Technological Changes Affect Libraries

The computerization of librarians and archives poses problems for several reasons: (1) there tends to be more information being accumulated and preserved with computers than without; (2) there are more points of access, therefore, more points to be controlled; and (3) more people are able to share the same material that has been placed into a computer data bank than is possible when only one or several hard copies are available. Hence, with computerization there is more need for monitoring of confidentiality safeguards than with manual files, yet science has not yet given us adequate protective technology.

For example, networks which allow more and more individuals to access the system at the same time compound the problem. Computerized reference service networks are especially vulnerable. For instance, a program in California funded by the National Science Foundation seeks to determine if libraries can be used as linking agents between the general public and information in computer data bases. This raises new issues of determining who uses computers to access what information.[20] Confidentiality takes on intensified concerns when an inquiry is of a sensitive nature, such as a request for planned parenthood information or information on a drug rehabilitation program.

There are already in existence today long-distance, high-speed, interlibrary facsimile links to keep scientists in one laboratory in touch with the literature resources of a distant facility. One particular service enables rapid access to scientific information and exchange of research documents over telephone lines between marine biology centers in Florida and Massachusetts. The digital facsimile transceivers by Rapicom[21] link not only the 170,000-volume, 2300-medical journal library of the Health Center at the University of Florida's main campus in Gainesville, Florida, with the C.V. Whitney Laboratory for Experimental Marine Biology and Medicine on the Florida coast five miles away, but also with the Marine Biological Laboratory in Woods Hole, Massachusetts.

One of the more difficult areas in terms of issues of professional ethics and the rights of a user to know is in the area of medical research questions. Often the librarian is trapped between trying to determine whether to provide information to the user consistent with the role of librarian, or whether to refer the question to a medical doctor. Generally, librarians view their role as that of providing information wherever possible, provided they are not called upon to make diagnoses or judgments that are more appropriately the domain of a medical doctor. Some libraries may have their staff prepare answers to medical questions but do not open their medical collections to the public. An interesting recent survey showed that 82 percent of the publicly funded medical school libraries are open to the public. Thirty-two percent offer public services other than access.

The kinds of developments which increasingly pose disturbing potential threats to the confidentiality of sensitive data have prompted a strong professional response from librarians. The American Library Association adopted a "Policy on Confidentiality of Library Records" in 1971 and amended it in 1975. The policy statement sets forth three basic principles for the guidance of its members: (1) the obliteration of all patron records when there is no longer a bona fide need for them;

(2) the use of an identifier other than a social security number; and (3) the development of safeguards to eliminate unofficial monitoring of communications channels used in library research.[22] The problem with self-regulation through professional training and codes of ethics, however, is that an increasing number of library personnel are nonprofessional employees. Also, given the special vulnerabilities that computerization brings, the expectation of voluntary compliance spearheaded by librarians may be naïve.

Given these kinds of problems, the Privacy Commission recommended many different actions. Although the specific recommendations of the commission total over 160, they embody only a handful of guidelines and principles to be applied to all information involving people. The goals of the Privacy Commission are threefold: (1) to minimize intrusiveness, (2) to maximize fairness, and (3) to create a legitimate and enforceable expectation of confidentiality where such expectation is warranted.

To accomplish these objectives, there are certain principles to which administrators should adhere. First, they should develop an appropriateness test for the collection of information; second, they should provide the protection of confidentiality; and third, they should guarantee the right to disclosure. Only information that is relevant to the decision at hand should be collected, and it should only be used for that purpose. Before an organization transfers these data to a third person, it should obtain the approval of the person whose record it is. The individual should be informed which sources will be contacted to get information, how the data will be used, and to whom the data will be disclosed. No information should be obtained under false pretenses, or through the impersonation of others. All individuals should have the right to see and copy records about himself or herself from any organization that keeps a file on the individual, including an employer. If the individual questions its accuracy, the person should have a right to correct the record. Where the point is in dispute, the individual's statement of his/her position should be made part of the permanent file. Secret files should be outlawed, so that individuals always have knowledge of the existence of records on them.

Government officials who want to gain access to a person's records should be required to present proper authorization before being permitted to do so, and the person should be notified when such disclosure is made. Organizations should only employ service and support firms whose privacy standards and principles are equivalent to their own.

**Confidentiality and MRDF**

Alice Robbin, president of the International Association for Social Science Information Service and Technology, has written:

> Some of the statistical and research activities of the social scientist have depended on access to and use of information on data subject in individually identifiable form. Similarly, some of the information collected by official data-gathering agencies for their research, statistical, accounting, or administrative purposes has the potential for increasing intrusiveness and harm by parties either associated or unassociated with the original data gathering effort, through compulsory, advertent, or inadvertent disclosure.[23]

The Privacy Protection Study Commission addressed this issue, and observed that activities of the social scientist have depended on voluntary cooperation of the individuals in providing accurate and reliable (confidential) information, with assurances that the information will not be released by third parties in individually identifiable form[24] in a manner whereby inadvertent or unauthorized disclosure of the information would place the data subject at risk.

The accumulation of machine-readable data files (MRDF) on human subjects by government agencies for administrative functions provides much rich data for the social scientist. The Privacy Commission recognized this and recommended to protect an individual

> from inadvertent exposure to an administrative action as a consequence of supplying information for a research or statistical purpose...[and] to protect the continued availability (supply) of research and statistical results which are important for the "common welfare," ...there must be a clear functional separation between research and statistical uses and all other uses....The principle must be established that individually identifiable information collected or compiled for research or statistical purposes may enter into administrative and policy decision making only in aggregate or anonymous form. The reverse flow of individually identifiable information from records maintained by administrators and decision makers to researchers or statisticians can be permitted, but only on the basis of demonstrated need and under stringent safeguards.[25]

Thus official data-gathering agencies must develop a "specific set of standards and guidelines for...practices [which] limit...exposure to risk of the individual who contributes information, either directly or indirectly, to a research or statistical activity,"[26] and which, moreover, distinguish among different types of information and types of release. Data librarians who collect, organize and disseminate the contents of MRDF, many of them issued by various government bodies, have dem-

onstrated recognition of the ethical considerations which must come into play when striking a balance between the individual's right to privacy and society's need for knowledge. "Proposed ethical standards" for data archivists and data librarians which treat these concerns have appeared in E. Mochmann and P. Müller's recent volume *Data Protection and Social Science Research: Perspectives from Ten Countries.*[27]

Although the Privacy Commission did not single out the library or archival function for a specific set of recommendations, it did make such recommendations for the related function of research. These follow the same general principles described earlier. These recommendations, in the form of several different pieces of legislation, are now proceeding through Congress.

**Research Activities Recommendations**

In view of the previous discussion, six recommendations for research activities can be made.

First, records and information gathered for research purposes should never be used to influence any decisions or actions directly affecting one of the individuals surveyed, unless that person so authorizes their use. Research organizations should establish a special set of rules to ensure that this will not happen. This means that there should be technical, administrative and physical safeguards against unauthorized or inadvertent disclosure, and the information should be rendered anonymous by being stripped of identifiers as soon after collection as possible.

Second, the organization conducting the research may only disclose individually identifiable records without the consent of the individual identified if certain conditions are met:

1. such disclosure is necessary to accomplish the purpose of the undertaking,
2. the disclosure yields enough social benefit to warrant the increase in the risk to the individual of such exposure,
3. safeguards against unauthorized disclosures are established, and
4. further use or redisclosure without the express consent of the individual identified is prohibited.

Third, no one should be required to divulge information about himself or herself for a research or statistical purpose unless the law requires it. To ensure this, the individual should be informed:

1. that his or her participation is at all times voluntary;

2. that the data collection has a specific purpose, and what this purpose is;
3. that there is a possibility that the information may be used in individually identifiable form for additional purposes, research or not; and
4. that if disclosure for purposes other than research is required, the individual will be promptly notified.

Fourth, there should be a review process or a special representative in every research organization responsible for applying the above principles in special cases, specifically, in order to protect people who are not competent to give consent for fear of some loss of benefit or some potential retaliation (for example, prison inmates, employees, welfare recipients, or students). Also, this process should provide safeguards in cases where the research requires that the people being studied are unaware of the existence, purpose or specific nature of the research.

Fifth, if and when these guidelines are followed, an individual should have access to whatever information is used or disclosed in individually identifiable form for any purpose other than a research or statistical one (for example, an inadvertent unauthorized disclosure). Fairness demands that people be able to find out what individually identifiable information about them has been made available. Of course, the research organization should keep an accurate accounting of all such disclosures.

Sixth, if any of the information is disclosed without an assurance that it will not be used in any decision or actions directly affecting the individual concerned, or without a prohibition on further use of disclosure (for example, to a court or an audit agency), the individual should be notified of the disclosure and of his right to access to the record.

The Privacy Commission urged the implementation of these principles; it did not recommend the creation of another regulatory agency to enforce them. Rather, the commission recommended that individuals be given the right of action against persons and organizations who violate these principles. Such legal action would be not only for court costs and actual damages, but also for general damages of between $1000 and $10,000.

## Conclusion

The substance of these privacy recommendations is to chip away at the centuries-old property right that organizations have always asserted toward the personal information they maintained in their files about individuals. It is the belief of the Privacy Commission that the time has

come to create an enforceable claim which the individual can assert to gain access to his or her records. There may be concerns that these privacy protections are too extreme or that they will interfere with the efficient administration of a library or a business. These changes may be viewed as yet another unnecessary drag on the day-to-day operation of commerce.

The goals of efficiency and privacy are not mutually exclusive. Those who think there is a basic conflict between long-term management effectiveness and safeguarding personal privacy rights must either be inexperienced in the art and science of management or ignorant of the consequences of personal privacy abuses. Personal privacy protection is as necessary to the vigor of a successful organization as it is to a nation. One of the significant features distinguishing a totalitarian regime from a democratic one is the deprivation of the individual's right to privacy. Over a century ago, de Tocqueville warned, " 'If the private rights of an individual are violated...the manners of a nation' are corrupted, putting 'the whole community in jeopardy.' "[28]

The findings of the Privacy Commission, as well as recent research at the University of Illinois, produced evidence that the private rights of the individual are currently being violated in the United States. Further, public opinion polls reflect this. A Harris survey released in December 1978 revealed that 64 percent of the people are concerned about threats to their personal privacy, up from 47 percent one year earlier.[29] Thus, until a comprehensive federal privacy policy takes shape, it is up to libraries as organizations to assume the responsibility of examining their practices for abuses of privacy, and voluntarily modifying, if necessary, their policies and procedures.

## References

1. Warren, Samuel D., and Brandeis, Louis D. "Right to Privacy." *Harvard Law Review* 4(15 Dec. 1890):193. (They stated, "And now the right to life has come to mean the right to enjoy life—the right to be alone." [This was in contrast to early interpretations of the right to privacy as the right to life.])

2. *U.S. Statutes at Large*, vol. 88, P.L. 93-579; "Privacy Act of 1979," 5 *U.S. Code*, 552a; and Privacy Protection Study Commission. *Personal Privacy in an Information Society*. Washington, D.C.: USGPO, 1977.

3. Linowes, David F. "The Impact of Computer Technology on Personal Privacy." *Scientific American*, in press.

4. Ibid.

5. From speeches presented at the International Conference of Data Commissioners, Ottawa, Canada, 22-24 Sept. 1980.

6. Crawford, Miriam I. "Access and Confidentiality." In *Archive-Library Relations*, edited by Robert L. Clark, Jr., p. 23. New York: Bowker, 1976.

7. *See* excerpts of the Society of American Archivists Policy on "Standards for Access to Research Materials in Archives and Manuscript Repositories." In *Access to the Papers of Recent Public Figures: The New Harmony Conference*, edited by Alonzo Hanby and Edward Weldon. Bloomington, Ind.: Organization of American Historians, 1977.

8. Hofferbert, Richard I. "Social Science Archives and Confidentiality." *American Behavioral Scientist* 19(March/April 1976):484; and Robbin, Alice. "Ethical Standards and Data Archives." In *Data Protection and Social Science Research: Perspectives from Ten Countries*, edited by Ekkehard Mochmann and Paul J. Müller, p. 218. Frankfurt: Campus Verlag, 1979.

9. Garwood, Alfred. "The Confidentiality of Library Records." *New Jersey Librarian* 9(March 1976):6.

10. "FBI Requests Library Records." *Newsletter on Intellectual Freedom* 24(Jan. 1975):27.

11. Ibid.

12. "Poetic License." *American Libraries* 10(June 1979):286.

13. "Policy on Confidentiality of Library Records." In *Intellectual Freedom Manual*, pt. 2, edited by Office for Intellectual Freedom, ALA, p. 31. Chicago: 1974.

> The Council of the American Library Association strongly recommends that the responsible officers of each library in the United States:
> 1. Formally adopt a policy which specifically recognizes its circulation records and other records identifying the names of library users...to be confidential in nature.
> 2. Advise all librarians and library employees that such records shall not be made available to any agency of state, federal or local government except pursuant to such process, order or subpoena as may be authorized under the authority of, and pursuant to federal, state or local law relating to civil, criminal or administrative discovery procedures or legislative investigatory power.
> 3. Resist the issuance or enforcement of any such process, order or subpoena until such time as a proper showing of good cause has been in a court of competent jurisdiction. Point 3,...means that upon receipt of such process, order, or subpoena, the library's officers will consult with their legal counsel to determine if such process, order, or subpoena is in proper form...; or if good cause has not been shown, they will insist that such defects be cured. (Adopted 20 Jan. 1971 by the ALA Council.) Revised 4 July 1975.

14. Funk, Roger L. "You are What You Read." *Privacy Journal* 6(May 1980):3.

15. Ibid.

16. Ibid.

17. Ibid.

18. Ibid.

19. Ibid.

20. Kuney, Joseph H. "A Publisher's Viewpoint." *Bulletin of the ASIS* 1(Oct. 1974):20.

21. *Newsletter, Advanced Technology Libraries* 9(Oct. 1980):1.

22. "Policy on Confidentiality," p. F-4.

23. Robbin, "Ethical Standards," pp. 215-16.

24. Privacy Protection Study Commission, *Personal Privacy*, chap. 15.

25. Ibid., p. 573.

26. Ibid., p. 574.

27. *See* Robbin, "Ethical Standards," pp. 214-22.

28. De Tocqueville, Alexis. Quoted *in* David F. Linowes. "Must Personal Privacy Die in the Computer Age?" *American Bar Association Journal* 65(Aug. 1979):1184.

29. Louis Harris and Associates. *Dimensions of Privacy* (National Opinion Research Survey of Attitudes Toward Privacy poll conducted for Sentry Insurance Company). New York, 1978, p. 5.

This Page Intentionally Left Blank