67th IFLA Council and General Conference
August 16-25, 2001

Code Number: **145-83-E**
Division Number: **0**
Professional Group: **Committee on Copyright and other Legal Matters**
Joint Meeting with: -
Meeting Number: 83
Simultaneous Interpretation: **Yes**

Privacy in the Digital environment—issues for libraries*

Michael Gorman
Dean of Library Services
California State University, Fresno, USA

Introduction

I published a book on library values[1] last year in which, based on extensive readings in both axiology and librarianship and on the experience of 40+ years work in libraries, I formulated and discussed eight "core" values—one of which is *Privacy*.

What is the meaning of privacy?

I sometimes think that "privacy" is in the ear of the listener. Certainly, there is by no means a universally accepted definition of the word. In Webster's Third, "private" is defined as "belonging to, or concerning, an individual; personal; one's own …"[2] Private things, therefore, belong to the individual—they are her or his personal property. In a free society, the things that belong to you legally are inalienable and cannot be removed or interfered with without your permission. We all need privacy in a spatial sense and an informational sense. Our spatial privacy gives us the right to be alone, to associate only with those with whom we choose to associate, and to be free from surveillance. Our informational privacy is the right to control personal information and to hold our retrieval and use of information and recorded knowledge to ourselves, without such use being monitored by others. We also have the privacy that is embodied in the term "private property"—those things that we own, including intangible, intellectual private property. The rights to privacy that seem so obvious to us in our daily lives are not always legally guaranteed or practically achievable—particularly in the technological context of today.

---

* **ADAPTED FROM A CHAPTER IN THE AUTHOR'S** *OUR ENDURING VALUES*. CHICAGO: ALA, 2000

1. Gorman, Michael. *Our enduring values*. Chicago: ALA, 2000.

2 *Webster's Third new international dictionary of the English language*. Springfield, Mass. : Merriam, 1976.

What has technology wrought?

Technology is neither good nor bad in and of itself. Technological advance may contribute to societal progress or may be a detriment to society or may be both (just think of advances in fertility medicine in a world that contains 6 billion people) or may be neutral. It is a natural human tendency to personalize technology in general and specific applications of technology. For instance, how often have you heard someone say "I hate cell 'phones"? The truth is that large numbers of us do not "hate" cell 'phones; they dislike the intrusive misuse of them by boors, bores, and solipsists. It is the human use and misuse of technology that arouses the emotions and it is the human use and misuse of technology that we should observe, study and seek to amend for the better.

It often seems that every advance in technology exacts a counter-balancing price or detriment. There is no such thing as a free technological improvement. Possibly the most obvious price that we are all paying is the actual and potential erosion of privacy caused by the compilation of, and easy access to, large and complex databases resulting from commercial, governmental, and non-profit transactions. The latter, of course, include transactions between libraries and library users and transactions that take place in libraries. Here are words to make us wary. "Every keystroke can be monitored. And computers never forget."[3] The same article quotes Marc Rotenberg, director of the Electronic Privacy Information Center:

With the new online services, we're all excited that this is going to be our window on the world, to movies to consumer services, for talking with [*sic*] our friends. The reality is that this may be a window looking in.

The point is that it is not technology that is the enemy of privacy but our joyful use of technology. We give away something of ourselves each time we engage in online transactions. Many people worry about potential governmental and commercial abuse of the information we are required to supply by law or in pursuit of a commercial transaction. Though these are real concerns, there is a wider picture that goes beyond the economic and governmental. We live more and more of our lives online and the accumulations of data about us grow ever larger while there is an ever-increasing ability to retrieve and manipulate that data speedily. We are coming to see that the history of society is cyclical and that cyberspace resembles nothing as much as a medieval village—a place in which privacy was unknown.

Electronic technology pervades government, commerce, and many forms of social interaction. We are right in being concerned about the integrity of our personal data and should support efforts by governments and others to devise regulations and codes that limit (but can never eliminate) incursions on that data. As long ago as 1973, the United States Department of Health, Education, and Welfare issued a code[4] on personal data systems based on the following (paraphrased) principles:

- no secret record keeping systems
- access to one's own records
- the ability of an individual to prevent data gathered for one purpose being used for another
- the ability of individuals to correct or amend their own records
- organizations collecting personal data must ensure its reliability and prevent misuse

It seems to me that those 25-year old principles still hold true in a very different computer world. They are even more difficult to enforce than they were then but they do provide the basis for humane and responsible collection and retention of personal data.

---

3 . McGrath, Peter. Info 'snooper highway.' *Newsweek* vol. 125, no.9 (February 27 1995) pp. 60-61.

4 . U.S. Dept. of Health, Education and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. Records, computers, and the rights of citizens. Washington, DC: GPO, 1973.

The history of privacy

In the Western world, privacy emerged as a social issue in the 18th century. Before then, people, even rich and powerful people, lived open lives because of the nature of society and the buildings in which they lived. Most people lived, ate, slept, played, etc., communally. Even more importantly in respect of privacy, there was little or no distinction between domestic life and work life. Reading and copying, for example, were communal activities in the Middle Ages. The concept of privacy and the solitary life of the mind came when communities and extended families gave way to nuclear families with houses with solid walls that contained separate rooms and were situated on private land. In the 18th and most of the 19th centuries, such houses belonged to the wealthy. Even then, communities persisted in the cohabitation of families and their servants. It was not until the 20th century that the opportunity for privacy was available to the less well off in Europe and North America. The important changes in the ways in which people lived and worked—notably the physical and psychological separation of work and "private life"—created a hunger for privacy that has been extended and asserted in a number of steps over the decades. One very important step in the United States was the publication of a paper by future Supreme Court Justice Brandeis and a colleague arguing "the right to be let alone."[5] That influential paper (more than 100 years ago) was spurred by fears of the intrusive capability of then new technologies—cameras, tabloid newspapers, telephones, etc. Brandeis was to argue later that wiretapping telephones was the equivalent of opening sealed letters.[6] In the United States, the legal definition of privacy has evolved and developed slowly in the years since Brandeis' plea for privacy. The important Supreme Court case *Griswold vs. Connecticut* 7 (which said that a right to privacy implicitly, but not explicitly, contained in the US Constitution, underlies the right of married couples to use birth control) was only decided in 1965. There are those who say that the judgement that legalised abortion in the US—*Roe vs Wade*—the most famous case decided on the basis of an inherent constitutional right to privacy—is constitutionally flawed for that very reason. In other words, they believe that the US Constitution only protects that which it lists explicitly. One could not possibly underestimate the effect on American society of an acceptance and application of that view.

There is a considerable body of opinion among constitutional lawyers and philosophers that the US Constitution was framed on the basis of natural law and natural rights that are inherent in an ordered society.[8] Given that is so, it is not hard to see that the US Constitution is capable of interpretation that goes beyond the exact words of that document to place natural rights in a modern context. Privacy is, of course, one of the natural rights that was understood in the late 18th century. Privacy has been a matter of great weight to the individual and to society as a whole for more than 200 years but the right to privacy is nowhere near as entrenched in American law and constitutional thinking as most people believe it to be.

Privacy has remained a hot political, legal, and societal issue throughout the 20th century, and, in one form or another, is still fought over today. All American social movements have been combated by, among other things, invasions of privacy. All the protagonists of the women's movement, the fight for racial equality, the struggle for literary and artistic free expression, and other such movements have been subject to surveillance and intrusion by US government agencies and other compilers of dossiers on private lives. It would be naïve to believe that such outrages no longer exist, but it would be cynical to ignore the advances in privacy contained in the law. That being said, unless we restrain the effects of technology, those hard won legal rights are in danger of being vitiated by forces that cannot be controlled by law.

---

5 . Brandeis, Louis and Samuel Warren. The right to privacy. *Harvard law review*. 1890.

6 . Cited in Tuerkheimer, Frank M. The underpinnings of privacy protection. *Communications of the ACM*. vol. 36, no. 8 (August 1993) pp. 69-73.

7 . Supreme Court decision US 381 (1965).

8 . Hamburger, Philip A. Natural rights, natural law, and American constitutions. *Yale law journal*. v. 102, no. 4 (January 1993) pp. 907-960.

The present and future of privacy

Technology, in the form of vast electronic records of online transaction of all kinds and the possibility of searching and retrieving personal data from those databases, is morally neutral. As noted before, people can use this technology for good or ill, for their own profit or in service of humanity. Our privacy is invaded daily—the task is to ensure those invasions are controlled and have benign outcomes. We have clear opportunities and dangers and should work to take advantage of the opportunities and reduce the dangers. In 1992, the American academic Alan Westin published a list of ten important trends in the protection of privacy.[9] The trends, which are holding up well in a rapidly changing world, include:

- joint ownership of personal information by individuals and institutions
- institutions may only use personal data with the consent of the individuals
- collectors of personal data will issue privacy codes
- storage and use of personal data will be regulated
- theft and misuse of personal data will be criminalized
- a US federal agency dedicated to the protection of privacy will be established

Many of Professor Westin's forecasts are proving to be accurate. One of them is not. It hard to see a federal agency of the kind that he envisages being established, not least because of the American distaste for central government oversight of personal matters. What has happened is the establishment of a seemingly ever-changing mixture of legislation, government regulation, and self-regulation. (A good example of the latter are the various American Library Association (ALA) policies and statements on privacy.)

A number of US federal agencies are actively involved in privacy issues. They include the Departments of Commerce; Health and Human Services; and Labor; the Federal Communications Commission; and the Federal Telecommunications Commission—each addressing medical, financial, telecommunications, Internet, etc., privacy issues in a piecemeal manner. There are a large number of federal laws affecting privacy. In 1999, the Privacy Exchange (maintained by the Center for Social and Legal Research (USA)—an organization devoted to the issue) listed the following:[10]

- Cable communications act (1984)
- Children's online privacy act (1998)
- Consumer credit reporting reform act (1996)
- Driver's privacy protection act (amended 1999)
- Electronic communications privacy act (amended 1997)
- Electronic funds transfer act (amended 1996)
- Fair credit reporting act (amended 1997)
- Family education rights and privacy act (1974)
- Freedom of information act (amended 1996)
- Privacy act of 1974
- Right to financial privacy act (1978)
- Telecommunications act (1996)
- Telemarketing and consumer fraud act (1994)
- Video privacy protection act (1988)

All these are complemented by a host of regulations, court decisions, state laws, local ordinances, and pending legislation. Outside the circle of governmental action at all levels, there are many voluntary

9 . *Abstracted in* Schroeder, Deborah. A private future. *American demographics*. vol.14, no.8 (Auguswt 1992) p. 19.

10 . National sector laws. www.privacyexchange.org/legal/nat/sect/natsector.html

agreements between and within public sector entities (including ALA and other library organizations). It is obvious that this is a multi-faceted problem—one that affects us all to a greater or lesser extent—and it is being addressed by many political and other agencies in the absence of a comprehensive public policy approach.

The complexity of the American approach is in stark contrast to the approach of the European Union, which has issued a *Directive on data protection (effective October 25th, 1998)* that is binding on all the members of the EU. This difference in approach means that there is no one US agency and no single body of law that can link to the EU's legal requirement that personal data about the citizens of those countries can only be transferred to non-EU countries that offer "adequate" privacy protection to that data.

Dealing with the EU directive would, of course, be far easier if there were, in the United States, a single federal law and a single federal government agency to which we could refer. In its absence, the US Department of Commerce has drafted a statement of principles[11] that echo some of the provisions of Professor Westin's 1992 publication. In summary, those principles are:

- *Notice*. An organization collecting personal data must inform the individuals involved of what they are doing and their rights.
- *Choice*. Individuals must be able to opt out of their data being transmitted to third parties.
- *Onward transmission*. Personal data can only be transmitted to third parties that subscribe to privacy protection.
- *Security*. Organizations collecting personal data must hold it secure against misuse, disclosure, destruction, etc.
- *Data integrity*. Personal data may only be used for the purposes for which it was collected.
- *Access*. Individuals must have reasonable access to the data that has been collected about them.
- *Enforcement*. There must be mechanisms (governmental and/or private) to ensure compliance with privacy principles. Those mechanisms must include recourse for individuals whose data has been misused, follow-up procedures to ensure remedies are being applied, and sanctions against organizations that violate personal privacy rights.

Given the increase in online transactions of all kinds, the great commercial value of personal data databases, and the increase in electronic technology capabilities, it is inevitable that privacy will continue to be a major issue and one that is more and more subject to government regulation and private sector codes and compacts.

What is the relation between privacy and libraries?

There is a great difference between the passive accumulation of personal data for a variety of legitimate purposes and the deliberate, active invasion of privacy. The former has potential for abuse, the latter is abuse. To my mind, the greatest scandal of the complex of scandals (real and invented) that afflicts the American political culture today is the wholesale and largely successful attack on the right to privacy. Letters are read, traps are laid, e.mails are reconstructed, bookstore records are happy hunting grounds for inquisitors, the most private aspects of lives are laid bare to be condemned and sniggered over, and the right to your own thoughts, your own relationships, and your own beliefs is trampled on by zealots and bigots. This is the world of 1984, the world of mind control, the world of mental totalitarianism. The confidentiality of library records and the confidentiality of the use of library resources are not the most sensational weapons in the fight for privacy but they are important, both on practical and moral grounds.

In practical terms, a lot of the relationship between a library and its patrons is based on trust and, in a free society, a library user should be secure in trusting us not to reveal and not to cause to be revealed what is

11 . International Safe Harbor privacy principles. Draft—April 19, 1999. www.ita.doc.gov/ecom/shprin.html

being read and by whom. On moral grounds, we must start with the premise that everyone is entitled to freedom of access, freedom to read texts and view images, and freedom of thought and expression. None of those freedoms can survive in an atmosphere in which library use is monitored and individual reading and library use patterns are made known to anyone without permission. It is very important that all libraries follow a policy that ensures privacy and that they take steps to educate everyone in the library in that policy. In this context, we should always remember that most people in most libraries interact with library staff and student assistants far more than with librarians. Knowing this, a library with a privacy policy that is not communicated to all who work in the library is just as bad as one with no policy at all.

There is a sad irony in the fact that pre-automated systems were far better at preserving the privacy of circulation and use records than their automated successors. Older readers may remember systems in which a book card and a user's card were matched for the time and only for the time that the book was borrowed. Once returned, the two cards were separated and not even Hercule Poirot could find any trace of the transaction ever having taken place. Now, an electronic circulation system will preserve all circulation and use records unless it is told not to do so. Most library systems are set to delete circulation information after the materials are returned, but how difficult would it be for a skilled person to restore those "deleted" records? It seems, sometimes, that computer records are forever, if one has the skill, the desire, and the time to retrieve them. In addition, many systems choose to maintain a record of the last library user to borrow something (for convenience if a checked-in item is found to have been damaged or mutilated)—a small but significant invasion of privacy. Libraries serve communities and communities breed gossip, nosiness, and prurience. Those who enjoy such things can easily find out who in their community has been reading about divorce, murder, diseases, dieting, dyslexia, and sexual variations. Is such a potential invasion of privacy worth the ability to track down library vandals?

Self-check

One technological innovation that is actually assisting the right to privacy is the "self-check" device. This machine enables the user to check out books and other materials on her own. I am not aware of any studies on the circulation patterns of self-check users as opposed to those who take their materials to a circulation desk. However, it would seem reasonable to assume that a library user with access to open shelves might feel freer to borrow "controversial" materials if assured that no one would see what she was borrowing. If this is true, such materials would go far beyond the obvious suspects—sexual content, etc.—and extend to, for example, materials on diseases, English professors borrowing Danielle Steele books, "happily married" people borrowing books on divorce, and musical snobs borrowing hip-hop records. The self-check machine, invented to speed up the circulation process, may well be a signal contribution to the library right to privacy.

Privacy and electronic resources

There is a serious problem of disparity of access to electronic resources. In the words of Elisabeth Werby:[12]

> … not all Americans are beneficiaries of the technological revolution. Indeed the Internet is "one of the more polarized aspects of life today in America." … Among the 'least connected' Americans are the rural poor, single parent and female headed households and young households …

The figures on the "digital divide" vary from one survey to another, but no-one disputes the existence of that gap. The public library is in a position to compensate for that gap (as are academic libraries—particularly state-supported institutions in communities that contain a significant number of the disadvantaged) by supplying free access and guidance in using that access. This means that the question

12 . Werby, Elisabeth. The cyber library: legal and policy issues facing public libraries in the high tech age. National Coalition Against Censorship. www.ncac.org/cyberlibrary.html

of privacy and confidentiality is an ineluctable and important issue for libraries—like it or not. We provide access to the Internet because we believe in giving access to all materials, but this particular case is so important because we are providing access to a vital part of modern life. If we are to come to terms with a society in which computer skills are highly esteemed and rewarded and if we are to give access to modern communications to those who would otherwise be shut out, we will have to deal with the many consequences of that service. Privacy rights, intellectual freedom rights, parental rights, and other issues attached to Internet access are there and have to be confronted.

There are many age-old problems connected with library privacy, but electronic resources and computer systems have introduced new dimensions to the struggle for confidentiality. Anyone who wishes can monitor the use of online journals, find out who gains access to which Web pages, set up "cookies" that create caches of information on sites visited and resources consulted, and do a myriad other things. Here is a news item from *USA today* (August 25th 1999):

> PALO ALTO, Calif. Privacy watchdogs are concerned about a "fun" new feature at Amazon.com [the online bookseller] that allows anyone on the Internet to find out what [*sic*] kinds of books, videos, and CDs employers at America's corporations are buying.

You do not have to be a paranoid to wonder a little, the next time you key in your name, address, and other details when ordering a book or video, about the uses to which those data may be put. The Amazon.com feature sounds harmless (not to mention boring) but the fact is that such services accumulate vast amounts of data in an effort to maximize sales (for example, I regularly get messages from them suggesting new titles that are similar to those I have bought before). The consequent fact is that mass of data is open to major violations of individual privacy.

Invasions of privacy are often done with good intentions, but everyone knows which road is paved with those. In the electronic arena, users and librarians have to act to mitigate invasions of privacy and to be always alert to the possibilities for snooping and more sinister uses of data about personal use of electronic resources. William Miller[13] quotes the chairman of Sun Microsystems as saying "You already have zero privacy—get over it," a breathtakingly candid acceptance of the 1984 implications of pervasive technology and a chilling indication of the attitudes of these modern robber barons. If he is right, then, surely, it behooves us to work even harder to preserve confidentiality at least in the area in which we work. Librarians should never agree to the loss of privacy and should work hard to preserve the privacy of the individual by enunciating principles, creating policies, and putting them into action. We need to develop more detailed privacy codes that are flexible enough to cover all kinds of library use in a rapidly changing technological environment.

Privacy in action

The American Library Association issued an "interpretation" of its *Library bill of rights*[14] that addresses these problems in very broad terms and provides what is, essentially, an overview of the issues and an ethical framework for library policies rather than specific practical steps to be taken. For instance, the interpretation states that "[u]sers have both the right of confidentiality and the right of privacy" but also says that library users must be advised that those rights may be threatened by the technical difficulty of ensuring security of electronic information on use. Therefore, a library formulating a privacy policy should not look to this document for the details of such a policy. That said, the document does provide a useful beginning and the following conceptual bases for a policy.

---

13. in *Library issues: briefings for faculty and administrators*. Vol. 19, no. 5 (May 1999), p. [4].

14 . Access to electronic information, services, and networks / American Library Association. 1999. www.ala.org/alaorg/oif/electacc.html

- each library should relate its policy to the needs of its own community and the environment in which it operates
- library users have a right to confidentiality and privacy
- the rights apply to minors as well as adults.

This latter point is central to ALA's stance on "filtering" (the attempt to block "undesirable" electronic resources by programs) in that, since minors are entitled to the same rights as adults, there is no excuse for depriving adults of access to information deemed "harmful" to minors. Some American public libraries have sought to square this circle by using filters on most public terminals by setting aside "unfiltered" terminals for use by adults and minors with parental provision. This is a serious invasion of privacy in that no-one should be forced to identify themselves or to use certain marked terminals in order to gain access to the electronic resources they want or need.

The first step in formulating a privacy policy for libraries in the light of the ALA principles is to define the many issues that center on privacy. In essence, the library has to answer the following questions.

- Are circulation and other library records always confidential?
- Is the right to privacy different for different media?
- Does the age or the status of a library user affect privacy?
- Have all library users the right to access to all forms of information and recorded knowledge without monitoring?
- Under which circumstances can privacy be abridged?
- How far must the library go to ensure privacy?

Let me translate each of these questions into concrete (and actual) American examples and essay some answers.

- Q: Can law enforcement officers have access to circulation records?
  A: Those records should only be made available on production of a subpoena.
- Q: Does the right to privacy about book borrowing habits extend to Internet use habits?
  A: Yes, and any automatic tracking of use should be deleted or aggregated so that details of individual use are lost. It is acceptable, indeed recommended, that library use data be aggregated so that statistics on the use of the library classes of person (children, graduate students, etc.) can be retained and analyzed, even though the use patterns of individuals are erased.
- Q: Is a parent entitled to know what her child is reading or viewing? Is a college professor entitled to know which students have checked out materials she placed on reserve?
  A: the first is tricky, but a parent who is entitled to know what her child is reading is not entitled to access to library records to gain that knowledge. The library is not a child's guardian or monitor, and parents should gain their knowledge about their children's reading habits from the children in an atmosphere of mutual respect. The second question is easy. No.
- Q: Can any user of the library use any library materials and resources (including sequestered collections and Internet terminals) in privacy and without supervision?
  A: Libraries often keep collections of controversial materials in supervised places for reasons of security (it should never be for reasons of morality). Access to those collections should be a freely available to all users as possible. The only reason for monitoring Internet use is in cases when there is a time limitation because of demand for terminals exceeding supply.
- Q: If a children's or school library holds a reading competition, can it publish the list of books read by the winners?
  A: Yes, *but* only with the permission of the winners themselves. This illustrates the point that mutual consent is a necessary precondition of any breach of the confidentiality compact between the library and its users, even for benign reasons.
- Q: Should a library install barriers, screens, etc., or special furniture (even if they involve significant expense) to ensure that only an Internet user can see what he is viewing on a library terminal?

A: Yes. Just as a library user can read any library book without others knowing what he is reading, that library user should also be given reasonable accommodation to ensure privacy of Internet use.

Library privacy plans need to be built on a combination of principle—the natural law right to privacy—and experience—the case studies that illuminate and exemplify a principle in changing and different circumstances. The example of law enforcement access to library records is a perfect example of principle and experience in balance. The principle is that library records are confidential. Experience and the greater good of society tell us that confidentiality can be breached if, and only if, a formal legal instrument such as a subpoena is invoked and produced. Some years ago, FBI agents interrogated a number of academic librarians about the reading habits of foreign scientists working in this country. Quite properly, librarians were not awed by the flashing of a badge and, in almost all cases, refused to answer such questions in the absence of a proper instrument of authority.

As the reader will have seen from the questions and answers above, privacy and confidentiality issues are more complicated today than they were before. The environment in which we live is one of a complex of laws, regulations, regulatory bodies, and private practices. All the more reasons why libraries, and everyone who works in them, should be alert to the right to privacy and the policies that ensure that right is assured. Before electronic technology had the major impact on libraries that we see today, privacy and confidentiality of library records and personal data on library users were relatively simple affairs. We now live in a world in which many issues connected with going online are "hot" and affected by political and religious views. Our privacy codes need to be updated so that we can deal with modern circumstances without ever compromising our core commitment to privacy as an important part of the bond of trust between libraries and library users. That bond of trust is a precious thing and one that we should do our best to preserve. In the face of the onslaught of technology, it is more than ever important to preserve human values and human trust so that we can demonstrate that we are, above all, on the side of the library user and that user's right to live a private life.