

Libraries at University of Nebraska-Lincoln
Library Philosophy and Practice (e-journal)

University of Nebraska - Lincoln

Year 2007

Privacy Policy Assessment for the
Livingston Lord Library at Minnesota
State University Moorhead

Stacy Voeller
Minnesota State University, Moorhead, voeller@mnstate.edu

**Privacy Policy Assessment for the Livingston Lord Library at
Minnesota State University Moorhead**

Stacy Voeller

Assistant Professor
Electronic Resources Librarian

Minnesota State University
Moorhead, Minnesota USA

Introduction

The mission of the Livingston Lord Library (LLL) of Minnesota State University Moorhead (MSUM) is to support the academic and cultural experience of our students, faculty, and citizens of this region and to encourage their active, life-long learning. LLL acquires and organizes resources and provides the services that sustain research, support curricula, teach critical thinking, advance information literacy skills, encourage reading, advocate intellectual freedom, and enhance thoughtful, informed citizenship (Livingston Lord Library 2006).

Formation of effective policies is essential to protecting intellectual freedom and supporting the academic and cultural experience of the MSUM community. LLL's current policy on confidentiality of patron records does not support this effort. Since the passage of the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, privacy of library users has been under attack, and that attack is proceeding secretly across our country. Confidentiality is an important and deserved right in a democratic society. Libraries, as the cornerstone of a democracy, bear the responsibility of upholding free and complete access to public information sources to ensure participation and accountability.

The American Library Association (ALA) affirms that confidentiality ensures an atmosphere in which citizens may exercise their first amendment rights to read and think and believe without fear of intimidation. Privacy is essential to the exercise of free speech, free thought, and free association and the courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. The library profession has a long-standing commitment to an ethic of facilitating, not monitoring, access to information. This commitment is implemented locally by libraries through their development, adoption, and adherence to privacy policies that are consistent with applicable federal, state, and local law. In a library, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Libraries have a responsibility to maintain an environment respectful and protective of the privacy of all users. ALA maintains that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship (2006).

This policy assessment was done to determine whether or not LLL 's existing policy on privacy and the confidentiality of library records is adequate or even functional. This study

focuses on the fundamental components of a privacy policy, uses data of surveys conducted of libraries regarding their privacy policies and the various implications of the PATRIOT Act, and examines existing privacy policies to ascertain if other libraries are currently doing enough to protect the privacy of their users. This assessment further strives to determine whether or not the privacy policy of the Livingston Lord Library is acceptable. If not, a suitable policy will be proposed.

History and Context

Privacy as a Fundamental Right

The idea of privacy is one of the primary foundations of both the Library Bill of Rights (<http://www.ala.org/ala/oif/statementspols/statementsif/librarybillrights.htm>) and the Librarian's Code of Ethics (<http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.htm>). Inherent in these documents of the profession is the concept that what library patrons are reading and checking out is their own personal and private business. Libraries in this country have been committed to these fundamental rights throughout much of their history. The right to privacy might not be as inherent a right as most think, and this notion of privacy has a long history in America. While the Supreme Court has adopted a broad, but not unlimited view of the right to privacy under the Bill of Rights, the United States does not have a unified federal statutory law generally protecting an individual's right to privacy. Instead, Congress has passed various laws placing limitations on the use of personal information.

Privacy is defined in Merriam-Webster's Dictionary as "freedom from unauthorized intrusion <one's right to *privacy*>." Although not explicitly mentioned in the U.S. Constitution as many believe it to be, a right to privacy has been held to be implicit in the Bill of Rights, providing protection from unwarranted government intrusion into areas such as marriage and contraception.

In 1890, Louis Brandeis and Samuel Warren in their essay, *The Right to Privacy*, believed it imperative that individual rights to privacy be recognized and upheld by the courts. In order for the common man to be free from the many stresses involved with an ever-changing and technologically advancing world, they felt "the intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury" (Warren and Brandeis 1890, 196).

William M. Beaney sought "to determine whether it is meaningful to speak of a constitutionally protected right to privacy and, if it is, to describe the meaning and scope of that right as used by the Justices" (1962, 213). Beaney further explained how "the right to privacy is not specifically mentioned at any place in the Constitution" (1962, 214) and further questioned how someone could "assume that the right to privacy is protected by fundamental law" (1962, 214). Beaney clearly demonstrates the lack of protection afforded the private citizen by law, pinpointing throughout the Amendments the minimal mention of privacy as it relates to searches and seizures.

In 1965, the case of *Griswold v. Connecticut* defined a constitutional right of privacy. The case centered on a Connecticut law prohibiting the use of "any drug, medicinal article or

instrument for the purpose of preventing contraception.” The Supreme Court struck down state laws forbidding the sale, distribution, and use of contraceptives on the basis of a newly articulated constitutional doctrine known as the “right to marital privacy.” In *Griswold*, the Court “first recognized that there are behavioral matters into which the government may not intrude specifically adult consensual marital sexual relations” (Helscher 1994). At last official recognition of the right of privacy as constitutional was addressed. Many arguments both for and against the idea of privacy as a right have been waged since this historic decision, but this case will forever remain on the books as defining the notion of privacy as a constitutionally protected idea.

Based on hearings in 1965 held by the House of Representatives Special Subcommittee on Invasion of Privacy, the Privacy Act of 1974 (Public Law 93-579) was passed. The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by Federal agencies, and “for the first time gave statutory recognition to a right of privacy, but did not define it” (Linowes and Hoyman 1982, 490).

Since the adoption of the Privacy Act of 1974, other federal laws, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996, and the Fair Credit Reporting Act, limit the collection and use of sensitive personal information by a variety of non-governmental institutions. Additionally, the Driver's Privacy Protection Act protects consumers from the public disclosure of their driving records. Another law, the Electronic Communications Privacy Act, makes it unlawful, in most circumstances, to intercept or disclose the contents of electronic communications, including e-mail. All of these various laws can be piecemealed together when attempting to historically document a right to privacy in the United States .

Right to Privacy Valued by Libraries, Librarians, and the American Library Association

The idea of a right to privacy is firmly rooted in the ethical tenets of the library profession. As a basic and fundamental principle, librarians have sought to protect user rights to confidentiality by guarding patron records from public scrutiny. What users read, check out, and research is guarded as private and confidential.

The right to privacy in a library is also implicit in ALA 's Library Bill of Rights, guaranteeing free access to library resources for all users and opposing any limitations on the right to an individual's exercise of free expression. A specific privacy interpretation of the Library Bill of Rights was adopted by the ALA Council in June, 2002. Through these two important documents, the Library Bill of Rights and the Code of Ethics, librarians fight to protect patron privacy and preserve our democratic society by promoting a diversity of viewpoints and ideas to support an informed, literate, and educated public.

ALA also adopted another document in its efforts to ensure confidentiality of users. The *Policy on Confidentiality of Library Records* was officially recognized in 1970. This policy was in response to attempts by U.S. Treasury Agents to access library circulation records. Since this time, ALA has also constructed new documents, including those referring to actions to take when a request for information is made by law enforcement officials.

The current policy of the MSUM Library on the Confidentiality of Records reads: “A library user's name or information sufficient to identify a user together with the subject about which the user requested information shall not be made available upon request by any person other than the user pursuant to Minnesota Statutes 13.40 Library Data, 1984” (Appendix A).

While this policy may have been sufficient in 1984 when enacted, it does not support the political climate of today.

Historically, the FBI and law enforcement have made a practice of visiting libraries for reasons of protecting national security and reasons surrounding the supposed protection of the American public. The adoption of the PATRIOT Act produced a much more far-reaching set of laws. Few who voted for the Act knew that among its provisions included one that gave FBI agents the authority to see what Americans read. Although it does not mention libraries specifically, the sweeping legislation gives the FBI power to seize all of the circulation, purchasing and other records of library users on no stronger a claim than an FBI official's statement that they are part of a terrorism investigation.

Until the PATRIOT Act, the FBI had the authority to obtain bank records, credit records and certain other commercial records only upon showing that the records requested related to a suspected member of a terrorist group. The PATRIOT Act expanded the FBI's authority in two ways. First, giving the FBI the authority to seize any records of any entity—including libraries. Second, Congress dropped the requirement that the FBI actually have some evidence that the person whose records it sought was a member of a terrorist group or otherwise involved in terrorism.

The FBI has a history of abusing its power: monitoring, keeping records on and infiltrating civil rights organizations, protest groups and others that had broken no laws but were considered controversial. Little has changed to prevent the FBI from abusing its powers again if left unchecked, and that is why this policy must be addressed.

History of Privacy at the Livingston Lord Library

At the MSUM Library there is no specifically documented history of the idea of privacy and the inherent idea of confidentiality of patron records. The very existence of policy itself at the Library is relatively new, with the initial handbook created in the late 1970s by Dr. Darrel Meinke, who at that time was the Dean of Instructional Resources.

Policies and their existence were first noted in minutes of 1964 in reference to a Policy for Seminar Rooms, and the first referral to an actual Policy Handbook was dated November 6, 1974. For those minutes, it was noted that “consideration at some future meeting ought to be given to the compilation of a complete policy and procedural manual for the Library. Suggestions should be made as to areas that ought to be covered” (MSUM Archives 1974). Finally, in 1979, there is a reference in the minutes of both 1979 and 1980 regarding the policies of the library, and from these findings, it can be deduced that by sometime in late 1979, a formally approved Policy Handbook was adopted.

Specific history on LLL policy 4.8 Confidentiality of Records is almost non-existent. In the 1983/84 Handbook, the entry reads: “4.8 Confidentiality of Records - As a general policy the names of patrons to whom materials are charged will not be released to other patrons.” Policy 4.8 remains the same in the 1984/85 copy, and then in a memo dated April 1, 1987 from Meinke, he asks the Library Faculty to consider proposed changes to the Handbook which includes the following: “4.8 Confidentiality of Records - REPLACE sentence with: “A library user's name or information sufficient to identify a user together with the subject about which the user requested information shall not be made available upon request by any person other than the user pursuant to Minnesota Statutes 13.40 Library Data, 1984” (MSUM Archives 1987).

After this one and only suggested revision to policy 4.8, the first Handbook in Archives containing this adopted revision is dated 1988/89, and the policy has not changed since then.

State law, as noted in the current policy, also addresses library records and data. Minnesota Statute 13.40 itself is also very short and only minimally refers to the idea of privacy of borrower information and habits. The lack of substance concerning the privacy of users and confidentiality of their records must be addressed. The PATRIOT Act potentially violates at least six of the ten original Bill of Rights, and grants broad new powers to law enforcement officials permitting them to sidestep or avoid entirely many traditional controls on the surveillance, investigation, arrest, and prosecution of civilians residing in the United States. Legislative history supports the notion of privacy, as does the history of changes made by the ALA in reaction to events of the times. LLL has made only slight changes to its own privacy policy, and has not kept current with changes made across the country, particularly in light of the PATRIOT Act.

Literature Review

The ideas of privacy and confidentiality are not new to libraries. There is much evidence on the web pages of the national association as well as in the literature of the profession that adherence to the ethics of librarianship and to the guidelines of protecting confidentiality are essential. At no point in this literature review was research uncovered to the contrary. While the literature supports and also provides justification for ensuring confidentiality, not much literature addresses what libraries are doing to deal with the topic, except in the few surveys conducted and used as data sources for this project.

Back in the “old days” of the Library Awareness Program, there was no gag order as there is today with the PATRIOT Act. Librarians could publicly speak about FBI visits, and there was even national news segments detailing these accounts. Gordon Conable (1990) describes the Freedom of Information Act requests filed by ALA and the information they have acquired because of those requests. This climate of government accountability is not automatically enforced today, and pre-9/11 literature definitely involves more instances of interactions with law enforcement and FBI agents than is reported today post-9/11.

There exists a vast amount of literature on the importance of privacy and protecting the confidentiality of library users. Scott Seaman (1994) discusses the implications of electronic circulation systems. He describes confidentiality as a relatively new concept, and that even though ALA encourages compliance, there is no penalty for not adopting confidentiality policies. He further discusses the implications of the new, sophisticated technology quickly becoming common practice in libraries, and the access it allows to private information.

As early as six years prior to the attacks of 9/11, discussion of ALA's encouragement of all libraries to enact policies defining confidentiality of library records was being addressed (Wilkes and Grant 1995). The article provides details of past visits by law enforcement entities into libraries, and examines how reference departments in academic institutions in Texas have addressed patron confidentiality. Responses to their survey strongly supported the very concept of confidentiality, while the actions of many of these libraries in regards to actually adopting a policy do not. Prior to the study by Wilkes and Grant, Mary K. Isbeli and M. Kathleen Cook (1986) also wrote about the non-compliance by libraries of adopting confidentiality policies.

Another recurring theme in the literature is whether or not libraries have confidentiality policies. Discussion seems to center on the importance of having such a policy, but there is actually little evidence they exist. Studies and surveys by Goodrum, Estabrook, and a study of Louisiana libraries by Jackman and Kegel continue to provide evidence that policy creation, revision, and/or adoption is not occurring even though information on what should be included in this policy is abundant. Michael J. Monaco's (2001) dissertation on creating a model privacy statement for web sites describes in great detail all aspects of any type of privacy policy creation. Running in a similar vein are articles pertaining to protocol to follow if approached by law enforcement. Mary Minow (2002) provides sound advice on how to handle court orders and subpoenas, and also supplies practical tips.

Anne Klinefelter (2004) further expands on the activism demonstrated by librarians regarding the PATRIOT Act. She also notes that while librarians are taking a stand, they are not at the forefront of the debate like organizations such as the Muslim Community Association of Ann Arbor and the Humanitarian Law Project. The mere strength in membership of ALA makes it a viable opponent, and ALA is making waves, but as pointed out by Klinefelter, more can be done.

While ours is a nation which values privacy over many other things, in a technologically oriented society, citizens of this country provide personal information on an almost daily basis without even thinking about what it is they are revealing. David McMillen (2004) discusses how various government entities share information with each other while also describing the various types of legislation put into effect to help protect privacy.

The idea that librarians are remaining passive about the implications of the PATRIOT Act is challenged by Ellen D. Gilbert (2005). ALA's urgency in encouraging libraries to adopt policy and take a stand has been evident, and this article also discusses the grant from the Carnegie Corporation of New York to finance the Goodrum Impact Study used for this project.

Another way libraries themselves and those businesses working closely with libraries are trying to enact change is by challenging the legalities of the PATRIOT Act. Alison Leigh Cowan (2005) discusses how an organization called Library Connection enlisted the American Civil Liberties Union to challenge the request they hand over records that might be of use in a counterterrorism investigation. To date, a judge in Connecticut has ruled that the nondisclosure order was keeping the consortium's officers and directors from exercising their First Amendment right to speak out, and the government has decided not to appeal this decision. This is a victory for proponents of the right to privacy and the protection of First Amendment rights. A very few other accounts can be found in the literature of FBI attempts to garner information since 9/11. Baird (2005) writes about one librarian's brush with police who were acting on a tip and trying to confiscate library computers.

Several studies have been conducted to determine whether or not libraries are following the advice of the literature. The most prominent study, *Impact and Analysis of Law Enforcement Activity in Academic and Public Libraries*, supports the notion that while libraries and librarians affirm the right to privacy, they have not done enough themselves to assure it (Goodrum 2005).

Methodology

Three different data sources were used for this policy study. First, a total of 30 current privacy policies were investigated, and chosen because of their presence on the Internet.

Second, a survey conducted of Illinois libraries was utilized because it garnered responses from libraries about their policies in a timely fashion after the events of 9/11. The third, a more encompassing survey, was studied because it was commissioned by the ALA on a national level and was necessary for inclusion to ascertain if libraries had made progress on changing their policies. Of these two studies, only information regarding academic libraries has been included.

Current Privacy Policies

There was no clear-cut method design for choosing the policies of the 30 schools. The libraries were divided into three groups based on their size encompassing 10 small academic libraries, 10 medium-sized libraries considered to be peer institutions to MSUM, and 10 large research-sized libraries. A decision was made to garner a sampling from academic institutions of three sizes to see if the larger the school and presumably the resources, the more involved and in-depth their policy would be. Larger typically also means more staff potential for updating policies whenever necessary.

The second main consideration was the ease of finding the policy posted on the libraries' web sites. One of the ideas behind policy creation is that it presents the opportunity to publicly display to the constituent what the library does, and which policies it adheres to, allowing users to determine if an entity is holding up its end of the bargain. Many, many hours were spent just finding these 30 policies. Therefore, an assumption is made that most libraries do not have such a policy in existence, or at the very least, do not publicly post their policies on the web.

Locating current library privacy policies, in most circumstances, was difficult. The purpose of this examination was to ascertain if changes were in fact made in light of the challenges that the PATRIOT Act potentially poses to libraries. Documentation was not maintained of how many library web sites were visited before the 30 total number of privacy policies were located. Many more did not have policies publicly posted as should be the case. Several direct email contacts were also made in an attempt to gather more policies, and this garnered three additional policies, but some replies indicated no such policy was available. Three other libraries within the state of Minnesota and the Minnesota State Colleges and Universities system were also contacted. None of these could produce a current policy.

Survey of Illinois Libraries in 2003

The second source of information for this study was a survey conducted in the state of Illinois in 2003 by Leigh Estabrook. This survey sought "to understand how public libraries' were responding to new security issues and to the events of September 11, 2001" (Estabrook 2003). The *Illinois* survey of 2003 was necessary for inclusion to discern if any trends were evident between attitudes and actions taken chronologically closer to the time of 9/11 as opposed to those occurring several years later. This survey itself is important because not many surveys have been conducted regarding the impact of 9/11 on libraries, and the timeliness of these survey responses is important to consider.

The method of collecting data for this survey included:

The Library Research Center surveyed all public and academic libraries in Illinois for which it had valid email addresses. The web-based survey was delivered by an email invitation sent on September 3rd, with a follow-up email reminder on

September 15th. Additionally, the LRC sent a paper mail follow up on November 3rd, 2003. The Library Research Center received a list of 795 public and 189 academic libraries. Of these, there were valid and unique addresses for 531 public and 148 academic library directors. Of those contacted, 465 (87.6%) of public and 120 (81.1%) of academic libraries submitted the survey. Although these response rates are unusually high, we believe it can be attributed to the importance of the survey content to library directors and the multiple modes (paper and web-based) employed. Furthermore, it must be noted that the response rates are for all Illinois libraries contacted--not the total number of Illinois public and academic libraries (Estabrook 2003).

This study was valuable because it solicited responses at a time when the events of 9/11 were at the forefront of many minds. The country was still trying to come to grips with what had taken place, and libraries were speaking out against the sections of the PATRIOT Act potentially infringing on the rights of privacy of their users. The response rate was high in this study, supporting the importance of the survey topic to libraries, and of libraries using it as a tool to express their concerns.

ALA Commissioned Survey in 2005

The third source of data came from the findings of a study called the *Impact and Analysis of Law Enforcement Activity in Academic and Public Libraries*, and this was used in order to explain the actions taken by libraries. This study was commissioned by ALA in 2005, and it proposed to “obtain descriptive information regarding the type of contact academic and public librarians have had with law enforcement agencies, and to obtain information about how the potential for law enforcement contact and contact itself has affected the management and operation of the academic and public library. The information that this study gathered is very important to libraries, librarians, the patrons of libraries, and federal, state, and local policymakers as each seeks to better understand law enforcement activities and impacts in academic and public libraries” (Goodrum 2005, 1).

According to the methodology as stated in the survey findings,

The study sought to obtain descriptive information regarding the type of contact academic and public librarians have had with law enforcement agencies, and to obtain information about how the potential for law enforcement contact and contact itself has affected the management and operation of libraries in the United States recently. The study utilized a national survey distributed to academic and public librarians over the web, as well as in-depth interviews with librarians and library leaders conducted between January and April 2005. This section will describe the sampling procedures, the survey instrument and interview protocol development, procedures used to distribute surveys and conduct the interviews, and information regarding the response rate (Goodrum 2005, 2).

Inclusion for participation in the survey of academic libraries was “developed using the 2004 Integrated Postsecondary Education Data System (IPEDS) academic file. This file lists 4200 entries for academic institutions, including community colleges, four-year colleges, and universities (not all of which have libraries). Duplicate addresses and non-U.S. institutional

listings were removed, leaving a list of 4008 libraries. All 4008 were contacted to request participation” (Goodrum 2005, 3).

The *Impact* survey was highly useful because of its relevancy. The questions asked in the survey, particularly those in reference to academic libraries, provided a strong set of data to determine the impact of changing legislation on the attitudes, workings, and day-to-day activities in libraries. The very nature of its currency proved to be a strong attribute.

Findings

Why are many libraries not following the model created by ALA? As the national organization of the profession, ALA has been a leader in the movement to fight for the rights of privacy for all citizens of the United States, and particularly the rights of their library users. ALA has done a noteworthy job of supplying the information libraries of all types need to write a proper privacy policy. Their guidelines are posted prominently on their web site and are freely available for dissemination. Links are also provided to existing model privacy policies of all different types of libraries. The website is a creation of ALA's Intellectual Freedom Committee, itself a leader in advocacy issues for ALA.

ALA's response to the USA PATRIOT Act has been strong and steadfast. ALA has issued its own Resolution on the USA Patriot Act and Libraries (<http://www.ala.org/ala/oif/statementspols/ifresolutions/usapatriotactlibraries.htm>) that includes urging that the “Senate bar the use of appropriated funds by the Justice Department to search library and bookstore records under Section 215, and that Congress pass legislation restoring the privacy rights of library users.” Furthermore, at the above listed website, ALA “opposes any initiatives by the U.S. government to constrain the free expression of ideas or to inhibit the use of libraries, and also urges librarians and other library workers, trustees and advocates throughout the country continues their efforts to educate their users on the impact of Sections 215 and 505 of the USA PATRIOT Act on libraries.”

Three methods of research were utilized for this study. The first encompassed scanning the Internet environment for privacy policies currently in place on academic library web sites. The second method, a survey conducted of Illinois libraries, was employed because it garnered responses from libraries about their policies in a timely fashion after the events of 9/11. The third survey was studied because it was commissioned by ALA and was necessary to ascertain if libraries had made any progress on changing or adapting their policies since the time of the Illinois study.

Current Privacy Policies

While there is plenty of literature concerning the need for privacy policies, the lack of existing policies is astounding. For those policies actually in existence, substantive information is lacking. Most policies studied contained less than ten sentences. One can ascertain that policies less than ten sentences in length do not have staff taking the time or making the effort to create or even investigate such policy creation.

Sentence length, while seemingly an unscientific indicator, does allow a quick scan of what policy information is included, and demonstrates whether or not effort has been put into true policy creation. It should be noted that of those surveys more than 30 sentences in length,

all but one included the four most noted aspects needed for a more appropriate policy in light of the PATRIOT Act.

Policies on the Internet were studied for length and content. Sentence length provided insight into whether or not changes have been made based on the recommendations of the ALA . The shortest policy was two sentences in length, the longest 49. Four specific areas were checked for inclusion:

- Does the policy mention the PATRIOT Act?
- Does the policy provide mention of law enforcement officials?
- Does the policy mention any form of court order, judicial order, or subpoena?
- Does the policy supply any protocol for what staff would do if they received a request for information?

Of the 30 total policies investigated, many, surprisingly, seemed to have not been altered since the passage of the PATRIOT Act. Policy length alone was studied to determine how involved the policies were and their elements of inclusion:

Sentence Length of Policy	Number of Libraries (30 Total)
Less than 10	14
Between 10 – 20	9
Between 21 – 30	2
More than 30	5

The following table shows pertinent items which should be addressed in a privacy policy, and how many times those items were addressed throughout the investigated policies:

Policy Items Addressed	Number of Policies (30 Total)
References to Law Enforcement	14
References to Court Orders or Subpoenas	21
References to the PATRIOT Act	11
Protocols in Place for Dealing with Requests	5

Of these results, only one Peer Institution and two Large Research Universities contained all four Policy Items

Overall, it can be surmised that many, if not all, of these policies can use further adaptation. Of all the policies studied, the policy from Porter Henderson Library at Angelo State University in San Angelo, Texas (<http://www.angelo.edu/services/library/policies/ppm12.htm>) was the most inclusive of the important aspects necessary for a privacy policy.

Survey of Illinois Libraries in 2003

In this study, 120 (81.1%) of 148 academic library directors responded. Several important questions and responses from the survey were:

- Question 4: Does the library have a formal (written) policy or set of guidelines on how to handle a search warrant or subpoena from law enforcement? Yes: 19 (16.0%) No: 100 (84.0%)
- Question 6: Has your library adopted or changed any library policies as a consequence of/or to address concerns related to the passage of the USA PATRIOT Act? Yes: 15(12.6%) No: 104(87.4%)
- Question 6a: In what areas has your library created or changed policies as a consequence of the USA PATRIOT Act?
 - Internet use policy: 5
 - Patron privacy: 6
 - Retention of library records: 10
 - No response: 105
- Question 8: Since 9/11/01 how many requests for information about patrons or circulation records have you received from any type of law enforcement official? Yes: 6(5.0%) No: 114 (95.0%) (Estabrook 2003)

As seen from the reported responses, some action has been taken in response to the events of 9/11, but surprisingly few in light of the potential ramifications of the PATRIOT Act.

Why has more not been done? What are libraries and librarians waiting for? According to information reported in this study, it seems many felt change was not needed and that current policies provided enough protection. The study also appeared to demonstrate that more important was the need to prepare procedural information in case a request for information was presented, and that "it may be that librarians feel that they need to be prepared to comply with the USA PATRIOT Act in case they are questioned by law enforcement authorities and at the same time are not enthusiastic about impinging upon library users rights to expression or privacy...In written comments librarians wrote that libraries changed their policies to reduce library records and to prepare for law enforcement queries.

The policy is actually more procedure than philosophy and provides the steps to be followed if a court order is presented. We also reviewed all of our practices regarding record and data retention to ensure that we do not maintain any unnecessary records or data and to compile a list to present to the law enforcement official to explain that the data they seek is probably not even available.

- We adopted a search warrant procedural guide, but no other policies were modified in response to PATIOT act.
- We reviewed our policies on Internet use and patron privacy but did not change them."
- We changed our procedures so to eliminate records that link to a patron's name whenever possible. For example, Internet use records are erased at the end of the day." (Estabrook 2003)

These very responses speak directly to the smallest of efforts to make change to existing policy regarding privacy of library users. Clearly, librarians are aware of the climate the PATRIOT Act has created, but have only done the minimum amount of change in light of it. The ALA recommends a complete privacy audit should be done to assure user rights are being properly protected.

ALA Commissioned Survey in 2005

This study, the first national and comprehensive examination of librarians' perceptions of law enforcement activity in academic and public libraries since the September 11 terrorist attack, was conducted in 2005. Important statistics gathered from the study include:

Figure 22: Academic Library Established Policies or Procedures for Requests for Information: Yes, the library has established policies or procedures for dealing with requests for information from law enforcement agencies and/or officials: 416 (47.9%) No, the library does not have established policies or procedures for dealing with requests for information from law enforcement agencies and/or officials: 452 (52.1%)

Figure 25: Academic Library Changes to Policies Regarding the Collection and Retention of Patron Information Since Passage of the USA PATRIOT Act: Yes, the library collects and retains *more* information about patrons than before the Act: 11 (1.3%) Yes, the library collects and retains *less* information about patrons than before the Act: 199 (23.1%) No, we have not changed any policies regarding the collection and retention of patron information: 651 (75.6%)

Figure 26: Academic Library Changes to Patron-Use Policies for Materials as a Result of the USA PATRIOT Act: Yes, the library has changed its patron-use policies for materials as a result of the USA PATRIOT Act: 45 (5.2%) No, the library has not changed its patron-use policies for materials as a result of the USA PATRIOT Act: 816 (94.8%)

Figure 37: Academic Library Number of Instances of Requests for Records and Other Items by Law Enforcement Agencies: All respondents answered that between zero and three times had a variety of requests been made of them. A total of 74 instances were reported totaling 8.9%. (Goodrum 2005)

An overview from the survey goes on to reveal that

overall there has been limited impact on public libraries as a result of law enforcement activities since October 2001. Clearly, there are some instances where policies have been changed, collections have been modified, and some libraries have been contacted by law enforcement agencies/officials. But interestingly, some 52% of respondents indicated that they have no policies for dealing with requests from law enforcement agencies. In addition, almost 54% of respondents indicated that in their library training for handling of requests or orders for information by law enforcement agencies and/of officials had not occurred. Thus, for some academic libraries changes and impacts have occurred after October 2001 related to law enforcement activities. But for the majority of respondents there has only been very limited if any impacts or changes (Goodrum 28, 2005).

Analysis focused on results from these two surveys to investigate library responses to the PATRIOT Act and whether or not policies have been altered. Many libraries noted in their survey responses they have made no privacy policy changes since September 11.

The *Impact* study by Goodrum provides general reasoning as to why more effort has not been made. Comments included, "Parallel to suggestions that patrons were lacking in a complete understanding of the law, some respondents also made comments suggesting a lack of information or misinformation at a personal, institutional or state level. One comment suggested that on a state level, changes had not been made. Librarians' own awareness of

what the PATRIOT Act encompasses may also be a reason why many libraries have not altered their policies. Libraries have always had to comply with requests from law enforcement agencies, but not in the same ways the PATRIOT Act requires. The general sense that one receives is that the PATRIOT act is “awful” from an abstract perspective, but ‘it doesn't really affect my library or patrons as directly as budget cuts and other day to day concerns.’ Personally, some librarians might feel very strongly about the potential for privacy loss, but professionally they feel more a compelling responsibility to deal with daily practical issues and problems” (Goodrum 2005, 30-35).

The study by Estabrook supports the findings in the *Impact* study. One of the questions asked read, "Does the library have a formal (written) policy or set of guidelines to handle a search warrant or subpoena from law enforcement?" Nearly one-third (29.3%) of public and 16.0% of academic libraries answered yes.” (Estabrook 2003) What this means is that most libraries responding to the survey have not revised their privacy policy to reflect changes necessitated by the PATRIOT Act.

All three studies clearly demonstrate that libraries are not doing enough to enact proper privacy policies. Not much in the bodies of these policies has changed to reflect the climate of post 9/11 and the USA PATRIOT Act. LLL is also not currently prepared to appropriately deal with a request for information by law enforcement or by any government official. A clearly defined policy can help to ensure proper protocols are followed and mistakes are not made. This study examines the issue and will propose an appropriate privacy policy for the MSUM Livingston Lord Library to adopt.

Are libraries aware of the potential implications of the PATRIOT Act on their libraries and their users? Research shows that while some have a vague notion or an inkling that implications exist, librarians have not fully invested the time and effort into making necessary changes to their privacy policies. Libraries and librarians do seem to understand changes and adaptations to their current policies are necessary, but had not done anything to that end at the time these surveys were conducted. In writing a new policy for the LLL , an ideal policy seemed to be out of the question when dealing with legal counsel for MnSCU, and took several months of negotiation. Many libraries cannot afford the time such an endeavor would take because they are short-staffed and have responsibilities they consider to be of higher priority.

Policy Alternatives and Evaluations

At this point, several different policy alternatives can be considered. Libraries can keep doing what they are doing, especially if their current policy on privacy and confidentiality has not been challenged. Another alternative is to make minor policy changes. At the very least, libraries should be checking to see if their state has made any revisions to its laws regarding privacy, and academic libraries should be keenly aware of changes made hierarchically in their organizations. Yet another option would be to make the use of materials in a library as anonymous as possible. Completely changing the way libraries do business today and avoiding the link between users and what they use is an interesting alternative. As with any policy assessment, complete elimination of the policy being researched is an alternative, and is also considered in this study.

ALA has compiled a comprehensive set of guidelines and of questions all libraries should be addressing and considering regarding their privacy policy ([Appendix B](#)). This list covers the key questions any library should be able to answer in their privacy policy. Issues

regarding how patron information is used, when and if information about patrons can be released without their consent and implications of potential law enforcement visits and how the library would handle such visits are just a few considerations.

Status Quo

Maintaining the status quo is always a policy alternative, but for these purposes, not efficient or responsible. According to the *Intellectual Freedom Manual* of ALA, "Written policies give the public a means to evaluate library performance and prove that the library is willing to be held accountable for its decisions. A well-written, board-approved policy will help disarm critics: unfounded accusations seldom prevail when the library's operations are based on clear-cut and timely written procedures that reflect thorough research, sound judgment, and careful planning" (2006, 418). Libraries have a responsibility to serve the best interests of their users, and leaving the policy as it currently reads, in most cases, is a disservice. Most library users are not even aware of the implications of the PATRIOT Act and libraries need to do a better job of keeping their constituents informed.

When contemplating leaving a policy as it is, libraries need to keep in mind the ALA guidelines for what a privacy policy should entail. Many of the policies located and used for this study and referred to in both the *Illinois*(2003) library survey and the *Impact*(2005) study are not even scratching the surface of what a policy should be. Libraries and librarians should speak out against this option, and should be working within their own systems to ensure some type of action is taken. The only roadblock to this should be finding the necessary amount of staff time to ensure a proper privacy audit is conducted and the appropriate stakeholders are consulted.

Minor Policy Alterations

Making very minor adjustments to the current policy is a viable option. Many library privacy policies do just that. At a minimum, policies should refer to their state statute. In the case of the MSUM Library, reference should also be made to the Board Policies of MnSCU. The MnSCU Board has just recently adopted Policy 5.23 Security and Privacy of Information Resources Policy (MnSCU Board 2006). Referring to the suggested policy guidelines of your entity's professional organization is also encouraged. The ALA web site provides a wealth of information for libraries to use, and libraries would be remiss not to make reference to this in their own policy. This option eliminates the necessity of giving in-depth explanation of the policy and its ramifications, possibly allowing libraries to take an easy way out and not commit to a well-thought out process for creating a firm policy.

When comparing this policy alternative to the ALA guidelines, at the very least it can be considered a step in the right direction. Adding even minimal details to an existing policy directly reflective of the potential implications of the PATRIOT Act can only be beneficial. While not ideal, this policy alternative is still much better than doing nothing. Even the implementation of minor policy changes mandates consulting legal counsel. With the complexity surrounding all types of privacy issues in today's technological society, expertise must be utilized to ensure any changes are legally sound. All stakeholders should willingly embrace this option as a potential solution for ensuring patron privacy.

Anonymous Library Cards

One new policy alternative might be the design of a new library card checkout system. This possibility is discussed in an article by Ben Ostrowsky who suggests libraries switch to using anonymous cards “as a way to protect libraries from legal actions. Anonymous cash cards, better known as gift cards, are already in existence. Using the same principle, libraries can issue a borrower card that uses cash, rather than personal ID information, as collateral. Because the library knows how to contact the owner of a card associated with a photo ID, it is willing to loan hundreds of dollars worth of material” (2005, 22). While this policy alternative is definitely interesting, it is not politically or economically feasible. Library users will not like the idea of having to deposit money to borrow materials, and libraries will most likely not be able to afford the technology to implement it. On the MSUM campus itself, and on many university campuses, the ID card for the entire university serves multiple purposes. Not only does the MSUM card serve as a campus ID card and a library card, but also enables entry into dormitories and campus buildings as well as serving as a meal card for students. The very nature of the usage of this card disallows for the potential of an anonymous card.

This policy alternative addresses many of the guidelines and over-arching questions posed by the ALA . Simple anonymity can eliminate the connection of a user to the materials they have borrowed from their library. Again, this option is not feasible for most libraries and their budgets, but it hopefully is an option that will be less costly in the future. Because of the cost issue alone and the complexities surrounding an entirely new card system, the major stakeholders would not embrace this option favorably.

Policy Elimination

Just as maintaining the status quo is always an option, so is complete elimination of the policy. In this case, it is not feasible or ethical to eliminate the policy. Users deserve to know the protections that are in place in their library, and libraries must maintain these policies. Publicly available and posted policies demonstrate that a library is telling users its guiding principles, and libraries that do not make these available are doing a disservice to their clientele.

This option is unacceptable. If libraries are going to present themselves as a cornerstone of a democracy, there will always exist a responsibility to protect the privacy of their users. Policy elimination or even minor policy alteration will not work in the post-9/11 world of today. The guidelines and list of questions presented by ALA is long indeed, but all of these must be discussed, thought about, and put into practice as much as possible to ensure the very principles of democracy are not further eroded by our own government. As was discussed previously with maintaining the status quo, libraries and librarians should reject this alternative, and all stakeholders should be against this option as well. Unfortunately, as many stakeholders are not even aware of the potential implications of the PATRIOT Act, the responsibility rests with librarians to ensure an appropriate course of action is taken; a well crafted privacy policy needs to be adopted.

Policy Recommendation

Policies are necessary for the operation of the library, and have been since their inception. The visits by the FBI and the IRS throughout the 1970s, 80s and 90s heightened the need for policies and procedures that protect the patron within each library. A library's official policy on confidentiality and its day-to-day procedures designed to protect the patron are on the

front lines in the battle for a patron's privacy. Harter and Busha state: "the profession requires careful formulation of policies defining the degree of confidentiality required for all types of library records and a precise definition of the subject matter about which unauthorized communication should be forbidden" (Wilkes and Grant 1995, 474). As these past visits demonstrate, the United States government has a history of attempts to acquire information about library users, and there is no reason to believe this kind of behavior will stop, particularly in light of the secrecy the PATRIOT Act allows.

Also with the passage of the PATRIOT Act, "the FBI was no longer required to show 'specific and articulable facts' of a nexus between a particular person and spying or terrorism. Although less exacting than Fourth Amendment probably cause, the FBI still had to link an individual to suspect activity, before gaining access to his records under the FISA. Section 215 eliminated the need for any particularized showing" (Ramasastry 2006, 12). Other concerns regarding the changes between law enforcement requests of the 70s and 80s compared to those since the PATRIOT Act include

the debate over Section 215 also highlighted concerns about chilling our ability to read and associate freely. Many scholars and jurists have noted that increased government surveillance can have a chilling effect on expression and political activity. Librarians and booksellers opposed Section 215 arguing that it would deter Americans from reading, speaking, and engaging in political discourse for fear that the government would monitor such activities and put such information into secret files. A related issue was Section 215's gag order. People and organizations that received Section 215 orders cannot speak about them to the public. Section 215 surveillance occurs in secrecy. Civil liberties advocates emphasized that it is important to allow the recipients of Section 215 orders to speak freely. This promotes transparency in government and open debate on the Act (Ramasastry 2006, 12-13).

This very transparency in government is what forces those in power to operate under a set of checks and balances protecting the rights of American citizens. Those are the rights Americans are due, and should be upheld in a democracy.

ALA's own *Guidelines for Developing a Library Privacy Policy* (2006) provide a set of distinct and clear principles to follow when developing this policy. A library still must tweak and further adapt the guidelines to make them acceptable for their own organization, but this document provides a great overview and beginning. In drafting a policy for the MSUM Library, these ALA guidelines were closely modeled. Using this as a starting point, then existing policies were studied and examined for wording and ideas.

The MSUM Library should enact a new privacy policy. Everyone needs to understand and embrace the goals a privacy policy is seeking to implement, and "librarians should take pride in the profession's role in free speech through the commitment to the freedom to read, and staff should be willing and able to discuss these basic ethics" (Coyle 2002, 57). Most citizens have no idea of the ramifications of the PATRIOT Act Sections pertaining specifically to libraries without actually saying the word library, or of the Act's potential for attacking and invading their privacy.

The initial policy recommendation is attached (Appendix C), and this draft was submitted to the Minnesota State Colleges and Universities (MnSCU) legal counsel via email

communication. Distinct from the University of Minnesota, MnSCU “comprises 32 colleges and universities, including 25 two-year colleges and seven state universities ... The law creating the Minnesota State system was passed by the Minnesota Legislature in 1991 and went into effect July 1, 1995. The law merged the state’s community colleges, technical colleges and state universities into one system. Instead of three separate governing boards and three chancellors, there is now one board and one chancellor for the entire system” (MnSCU 2006).

After a number of revisions and consultation with legal counsel, a final privacy policy recommendation was drafted and is attached ([Appendix D](#)). Because MSUM falls under the over-arching guidelines of MnSCU, this policy draft reflects this hierarchy. Included wherever possible and allowed by legal counsel, this policy strives to include the essentials recommended by ALA including mention of the PATRIOT Act, visits by law enforcement, what information is collected, and applicable state and local laws. [Appendix C](#), as an ideal, includes all aspects of a good policy as recommended by ALA, but it is evident that the recommended policy as shown in [Appendix D](#) eliminates several aspects of this proposal as a consequence of direction from legal counsel.

While approval of this policy is the first step, acceptance must be combined with proper implementation. To ensure this policy is properly employed, the MSUM LLL must follow ALA guidelines. If the LLL does choose to enact this policy, librarians must thoroughly discuss and understand the new policy and attempt to foresee all possible implications. Training must be given to all library staff, and also to library student workers who typically the staff stationed at the public service desks. Staff needs to understand what to do if law enforcement does enter the building and seek particular information. Librarians must also be familiar with ALA 's various policies and guidelines on privacy, and must know what to do when faced with any type of inquiry, whether it is in the form of a court order, subpoena, or general request for information. Librarians, or any other party responsible for policy maintenance in the library, must be incredibly diligent about setting aside time for regular privacy policy evaluation and make any necessary updates or revisions to the policy based on changes to legislation surrounding privacy or changes to the PATRIOT Act. This type of endeavor should be undertaken for all library policies, but particularly for those concerning privacy which hold potential for change on a frequent basis. Ultimately, it should be the responsibility of library and university administration to ensure policy evaluations such as this are conducted regularly.

The ALA Code of Ethics (<http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.htm>) clearly lists privacy as its third principle. As professionals, librarians have a responsibility to uphold these ethics in securing rights of privacy for their users. Not doing so would be an ethical and professional violation. Library users depend on librarians, whether knowingly or not, to protect their right to privacy, and librarians must conscientiously work to uphold these tenets.

Conclusion

As recently as the 1970s and 80s, the FBI conducted a Library Awareness Program which investigated what library patrons were using, and it was something that (once librarians learned of it) became a rallying cry for librarians across the country against this type of secretive invasion. Librarians openly spoke out against the surveillance and attempts to gather information conducted by the FBI and law enforcement. Evidence of the chilling effect of the PATRIOT Act is much more difficult to find due to the gag order placed on libraries and librarians about when requests for information are made. Maybe this is the reason for the

seemingly passive role many libraries have taken regarding changing their confidentiality policies to protect the rights of their users.

The PATRIOT Act alone should not be the only impetus pushing libraries into revamping and strengthening their confidentiality policies. The very computer-centered society we have become is justification enough. Not only are libraries centers for technology for many, but “in today's world, everyone needs to know about the privacy implications of everyday activities like using a grocery store discount card or visiting the doctor...Libraries are the focal point for modern literacy needs, from reading to computer use, and they can play a key role in promoting "privacy literacy" by making information on privacy issues available” (Coyle 2002, 57). Libraries can and should play a key role in this potential information divide and must strive to help their users in any way they can.

Coombs (Coombs 2004, 497) provides three important action points all libraries should engage in. They are: “First, all libraries must have a suite of policies relating to privacy ... Second, libraries must educate their users concerning privacy issues ... Third, individual library privacy policies and association guidelines need to be more responsive to technological changes”. To truly protect user's privacy, libraries must ensure an environment of confidentiality, and these points are a step in that direction.

By denying access to information, which has ultimately always been considered a public good, the PATRIOT Act and the secrecy surrounding attempts to gather records on patrons, our own government prohibits an informed citizenry of their due process, and of any method of redress for things in which they are being investigated. This allows “the government to be an information holder, and the American public to be an information have-not” (Shuler 2005, 63).

Libraries must do whatever they can to promote, protect, and be vigilant about the need for privacy in a democratic society. Libraries and librarians must be willing to go to battle for this seemingly obvious piece of freedom in order to protect the right of privacy for those citizens who do not even fully understand the ramifications of potential governmental intrusion as allowed by the PATRIOT Act. Based on information from the Department of Justice's own disclosures, “federal judges had reviewed and granted the department's requests for a Section 215 order 25 times as of March 30, 2005 ” (Ramasastry 2006, 13), so there is some evidence, even with the gag order preventing those presented with a legal order, that a Section 215 has been issued. Libraries and librarians must protect privacy because confidentiality ensures an atmosphere in which citizens may exercise their First Amendment rights to read and think and believe as they will without fear of intimidation.

A meaningful and publicly posted privacy policy is the first step in removing barriers to information and of closing the information divide. Highlights of the recommended policy include, but are not limited to, information about state and federal privacy laws, reference to ALA documentation and to the policies and procedures of MnSCU. Also included is an explanation of what data are maintained, what type of information is retained in library files, and detailed information regarding what type of information can be collected via online visits to library web sites and related usage of online library services. In particular, the policy speaks to the four online areas of network traffic logs, web visit logs, cookies and information voluntarily provided such as the completion of an InterLibrary Loan request or submission of an Ask-A-Librarian form. Specific protocols are also given regarding requests from law enforcement and the steps the library will follow if such a request is made.

In the end, this privacy policy is much more specific than the original policy for LLL dating back to 1984. Because of the various factors surrounding the gag order with the PATRIOT Act, there seemingly is not enough evidence to support a rigorous privacy policy, but the very ethics forcefully upheld in the ALA Code of Ethics demonstrate that adherence to privacy protection is a right libraries and librarians must provide their users. At this point, almost any enhancement of the policy for the LLL is for the better, but the newly recommended policy covers many of the points strongly recommended by the ALA .

References

- American Library Association. 2005. "Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff." <<http://www.ala.org/ala/oif/ifissues/guidelineslibrary041905.pdf>> (May 5, 2006).
- American Library Association. 2006. "Guidelines for Developing a Library Privacy Policy." <<http://www.ala.org/oif/iftoolkits/privacy/guidelines>> (May 5, 2006).
- American Library Association. 2006. "Privacy: An Interpretation of the Library Bill of Rights." <<http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/privacy.htm>> (May 15, 2006).
- American Library Association. 2006. "Resolution on the USA PATRIOT Act and Libraries." <<http://www.ala.org/ala/oif/statementspols/ifresolutions/usapatriotactlibraries.htm>> (May 29, 2007).
- American Library Association. 2006. "Suggested Procedures for Implementing 'Policy on Confidentiality of Library Records.'" <<http://www.ala.org/ala/oif/statementspols/otherpolicies/confidentialitylibraryrecords.pdf>> (September 23, 2006).
- Baird, Christine V. 2005. "Even the Libraries Can't Escape Expanded Powers to Spy." *The Star-Ledger*. 11 September, 1.
- Beaney, William M. 1962. "The Constitutional Right to Privacy in the Supreme Court." In *The Supreme Court Review*, ed. Philip B. Kurland. Chicago: The University of Chicago Press, 212.
- Brasch, Walt. 2002. "Ashcroft's Assault on Bookstores: The Fiction Behind National Security." July 25. <<http://www.counterpunch.org/brasch0725.html>> (February 1, 2006).
- Conable, G. M. 1990. "The FBI and you; did the FBI investigate you as part of its Library Awareness Program? Here's how to find out." *American Libraries*. 21 (March): 245-6.
- Coombs, Karen A. 2004. "Walking a Tightrope: Academic Libraries and Privacy." *The Journal of Academic Librarianship* 30(6): 493-8.
- Cowan, Alison Leigh. 2005. "A Court Fight to Keep a Secret That's Long Been Revealed." *New York Times*. 18 November, Sec. B.
- Coyle, Karen. 2002. "Make Sure You Are Privacy Literate." *Library Journal*. 127(16): 55-57.

Estabrook, Leigh. 2003. "The PATRIOT ACT and Illinois Libraries: A Report for the Illinois State Library." November. <<http://lrc.lis.uiuc.edu/web/PA.html>> (May 5, 2006).

Gansler, Jacques S. and William Lucyshyn. 2004. "The Unintended Audience: Balancing Openness and Secrecy. Crafting an Information Policy in the 21 st Century." September. <http://www.cpppe.umd.edu/Bookstore/Documents/UnintendedAudience_3.05.pdf> (May 4, 2006).

Gilbert, Ellen. 2005. "Confidentially Speaking: American Libraries and the USA PATRIOT Act." *Library Philosophy and Practice* 8(1): Online Journal, <<http://libr.unl.edu:2000/LPP/gilbert3.htm>> (May 17, 2006).

Goodrum, Abby. 2005. "Impact and Analysis of Law Enforcement Activity in Academic and Public Libraries." August 25. <<http://www.ala.org/ala/washoff/oitp/LawRptFinal.pdf>> (May 5, 2006).

Helscher, David. 1994. "Griswold v. Connecticut and the Unenumerated Right of Privacy." *Northern Illinois University Law Review* 15: 33-, from Online Subscription Resource Westlaw.

Isabeli, Mary K. and M. Kathleen Cook. 1986. "Confidentiality of Online Bibliographic Searches: Attitudes and Practices." *RQ* 25(4): 483-7.

Klinefelter, Anne. 2004. "The Role of Librarians in Challenges to the USA PATRIOT Act." *North Carolina Journal of Law & Technology* 5(2): 219-26.

Linowes, David F. and Michele M. Hoyman. 1982. "Data Confidentiality, Social Research and the Government." *Library Trends* 30(Winter): 489-503.

Livingston Lord Library, Division of Instructional Resources, Minnesota State University Moorhead . 2006. "Mission Statement." <<http://www.mnstate.edu/instructres/mission.cfm>> (July 31, 2006).

McMillen, David. 2004. "Privacy, confidentiality, and data sharing: Issues and distinctions." *Government Information Quarterly* 21(3): 359-82.

Minow, Mary. 2002. "The USA PATRIOT Act." *Library Journal* 127(16): 52-4.

MnSCU: About the System. 2006. "About the Minnesota State Colleges and Universities system." July. <<http://www.mnscu.edu/about/index.html>> (July 21, 2006).

MnSCU Board of Trustees. 2006. "5.23 Security and Privacy of Information Resources." April. <http://www.mnscu.edu/board/pending/04-policy3_23.pdf> (May 5, 2006).

Monaco, Michael J. 2001. "A Model Privacy Statement for Ohio Library Web Sites." Master's thesis. Kent State University .

MSUM Archives. 1964-2006. "Faculty Meeting Minutes."

Ostrowsky, Ben. 2005. "Anonymous Library Cards Allow You to Wonder, 'Who was that Masked Patron?'" *Computers in Libraries* 25(June): 21-23.

Ramasastri, Anita. 2006. "Why Are Librarians Mad About the USA PATRIOT Act?" *Insights on Law & Society* 6(Winter): 11-13, 25.

Seaman, Scott. 1994. "Confidentiality of Patron Records in Electronic Library Circulation Systems." Presented at the 18th Regional Conference on the History and Philosophy of Science Privacy and New Information Technologies, University of Colorado, Boulder.

Shuler, John. 2005. "Information Policy, A Post-Election Perspective: Whither Information Policy? Part Two." *The Journal of Academic Librarianship* 31(1): 63-66.

Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5): 193-220.

Wilkes, Adeline W. and Susan Marie Grant. 1995. "Confidentiality Policies and Procedures of the Reference Departments in Texas Academic Libraries." *RQ* 34(4): 473-85.

Appendix A. Minnesota Statute

13.40 Library and historical data.

Subdivision 1. Records subject to this chapter.

(a) For purposes of this section, "historical records repository" means an archives or manuscript repository operated by any state agency, statewide system, or political subdivision whose purpose is to collect and maintain data to further the history of a geographic or subject area. The term does not include the state archives as defined in section [138.17](#), subdivision 1, clause (5).

(b) Data collected, maintained, used, or disseminated by a library or historical records repository operated by any state agency, political subdivision, or statewide system shall be administered in accordance with the provisions of this chapter.

Subdivision. 2. Private data; library borrowers.

(a) Except as provided in paragraph (b), the following data maintained by a library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order:

(1) data that link a library patron's name with materials requested or borrowed by the patron or that link a patron's name with a specific subject about which the patron has requested information or materials; or

(2) data in applications for borrower cards, other than the name of the borrower.

(b) A library may release reserved materials to a family member or other person who resides with a library patron and who is picking up the material on behalf of the patron. A patron may request that reserved materials be released only to the patron.

Subdivision. 3. Nongovernmental data. Data held in the custody of a historical records repository that were not originally created, received, maintained, or disseminated by a state agency, statewide system, or political subdivision are not government data. These data are accessible to the public unless:

(1) the data are contributed by private persons under an agreement that restricts access, to the extent of any lawful limitation; or

(2) access would significantly endanger the physical or organizational integrity of the data.

HIST: 1980 c 603 s 21; 1981 c 311 s 39; 1982 c 545 s 6,24; 1991 c 319 s 3; 1992 c 499 art 10 s 1; 1996 c 440 art 1 s 7

Appendix B. Checklist of Basic Questions about Privacy and Confidentiality

Collecting Information

Do we need to know this to operate the library?

How long do we need to know it?

How will we protect what we collect?

How will we destroy what we collect?

How will we inform the public about confidentiality?

How will we give users choices?

How will we inform/influence government acts that impact confidentiality?

Providing Privacy

Where do users need privacy to protect their intellectual freedom?

Where would privacy endanger safety?

How will we provide privacy where we should?

How will we ensure safety without being intrusive?

How will we educate staff about privacy?

How will we inform the public about privacy in libraries?

How will we inform the public about library resources on privacy issues?

How will we give users choices?

Reviewing Your Policy

Does your policy statement explain the difference between privacy and confidentiality in a library setting?

Does your statement make clear the role of confidentiality in protecting intellectual freedom?

Is the information to be protected listed: reference requests, information services, circulation & registration records, server and client computer logs?

Have you included language to deal with unforeseen circumstances, like "including, but not limited to..."?

Does your policy require that library users be notified whenever their PII is collected by the library and be told how to correct inaccurate information?

Do you state who may or may not have access to patron information?

Do you outline the specific conditions under which access may be granted? i.e., with a court order after good cause has been demonstrated?

Do you list the procedure for adopting the policy?

Are there provisions for notifying the public of the policy?

Are exemptions, exceptions, or special conditions enumerated?

Do you address needs unique to your library environment?

If your library is part of a cooperative, automated library system, are there provisions for coordination with the other libraries in your system?

Is the procedure outlined for responding to court orders of various types?

Are the Library Bill of Rights, Statement on Professional Ethics, ALA Policy on the Confidentiality of Library Records, and state & local laws (where applicable) mentioned or acknowledged? Does your policy conform to these supporting documents?

Taken from ALA Web site <<http://www.ala.org/oif/iftoolkits/privacy/guidelines>>

Appendix C. Confidentiality of Library Records (Originally Proposed Policy to MnSCU)

Privacy is essential to the exercise of free speech, free thought, and free association. At the Minnesota State University Moorhead (MSUM) Livingston Lord Library, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy. Our library's privacy and confidentiality policies are in compliance with applicable federal, state, and local laws. The statute in Minnesota which pertains particularly to library data is [Minn. Stat. § 13.40](#). Because MSUM is a member of the Minnesota State Colleges and Universities (MnSCU) System, information can also be located on the [Board Policies](#) website. MnSCU is currently working to enact a privacy policy, and this can be viewed in the section under [Pending Policy Actions](#), with particular attention paid to [Proposed Policy 5.23 Security](#). Our Library also upholds the rights guaranteed our students in the [Family Educational Rights and Privacy Act](#) (FERPA) which was passed to protect the privacy of student education records and to define who can access these records, and the [Student and Exchange Visitors Information System](#) (SEVIS) which maintains updated information on non-immigrant foreign students and exchange visitors during the course of their stay in the United States each year.

Our commitment to your privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the [American Library Association's Code of Ethics](#): "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted."

Minnesota State University Moorhead Livingston Lord Library's Commitment to Our Users Rights of Privacy and Confidentiality

This privacy policy explains your privacy and confidentiality rights, the steps this library takes to respect and protect your privacy when you use library resources, and how we deal with personally identifiable information that we may collect from our users.

Notice and Openness

We affirm that our library users have the right of "notice"—to be informed about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of library services.

We post publicly and acknowledge openly the privacy and information-gathering policies of this library on our Web site at <http://www.mnstate.edu/instructres/policy/toc.cfm>. Whenever possible, we avoid creating unnecessary records, we avoid retaining records not needed for the fulfillment of the mission of the library, and we do not engage in practices that might place information on public view.

Information we may gather and retain about current and valid library users include the following (This list should be comprehensive, and should include locally relevant examples):

- User Registration Information is maintained indefinitely.
- Circulation Information is not kept in the form of a permanent ongoing record of borrowing for any individual. Once materials are returned, that record is deleted. However, the Library catalog's back-up files may retain borrowing information for up to 60 days after an item is returned.
- Electronic Access Information is not made available to any other entity outside the Library except as required by law. The Library maintains statistics only of database usage statistics. No records of visits from specific IPs are maintained.
- Information Required to Provide Library Services such as consultation services in the form of reference or research consultation are confidential and information about these services will not be shared outside the Library. InterLibrary Loan service necessitates the sharing of patron information between libraries, but will only be disclosed during these transactions if necessary to conduct Library business.

Choice and Consent

This policy explains our information practices and the choices you can make about the way the library collects and uses your information. We will not collect or retain your private and personally identifiable information without your consent. Further, if you consent to give us your personally identifiable information, we will keep it confidential and will not sell, license or disclose personal information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.

If you wish to receive borrowing privileges, we must obtain certain information about you in order to provide you with a library account. When visiting our library's Web site and using our electronic services, you may choose to provide your name, e-mail address, library card barcode, phone number or home address.

We never use or share the personally identifiable information provided to us online in ways unrelated to the ones described above without also providing you an opportunity to prohibit such unrelated uses, unless we are compelled to do so under the law or to comply with a court order.

If you are affiliated with our university, the library automatically receives personally identifiable information to create and update your library account from the Records Office (for students) or Human Resources (for employees).

Access by Users

Individuals who use library services that require the function and process of personally identifiable information are entitled to view and/or update their information. You must update your personal information with the Records Office (students) or Human Resources Office (employees) for it to take effect in your Library record. The purpose of accessing and updating your personally identifiable information is to ensure that library operations can function properly. Such functions may include notification of overdue items, recalls, reminders, etc. The library will explain the process of accessing or updating your information so that all personally identifiable information is accurate and up to date.

Data Integrity and Security

Data Integrity : The data we collect and maintain at the library must be accurate and secure. We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to your own personally identifiable data; updating data whenever possible; destroying untimely data.

Data Retention : We protect personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services.

Tracking Users : We remove links between patron records and materials borrowed when items are returned and we delete records as soon as the original purpose for data collection has been satisfied. Currently, the system default for all MnPALS Libraries is 60 days. We permit in-house access to information in all formats without creating a data trail. We do not ask library visitors or Web site users to identify themselves or reveal any personal information unless they are borrowing materials, requesting special services, registering for programs or classes, or making remote use from outside the library of those portions of the Library's Web site restricted to registered borrowers under license agreements or other special arrangements. We discourage users from choosing passwords or PINs that could reveal their identity, including social security numbers. We regularly remove cookies, Web history, cached files, or other computer and Internet use records and other software code that is placed on our computers or networks. The computers in the Library currently operate under a software program which reverts them back to their original state after two hours of inactivity. At a minimum, this process is done daily.

Third Party Security : We strive to ensure that our library's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. When connecting to licensed databases outside the library, we release only information authenticating users as "members of our community."

Cookies : Users of networked computers will need to enable cookies in order to access a number of resources available through the library. A cookie is a small file sent to the browser by a Web site each time that site is visited. Cookies are stored on the user's computer and can potentially transmit personal information. Cookies are often used to remember information about preferences and pages visited. You can refuse to accept cookies, can disable cookies, and remove cookies from your hard drive. Our Library servers use cookies solely to verify that a person is an authorized user in order to allow access to licensed library resources and to customize Web pages to that user's specification. Cookies sent by our Library servers will disappear when the user's computer browser is closed. We will not share cookies information with external third parties.

Security Measures : Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

Staff access to personal data : We permit only authorized Library staff with assigned confidential passwords to access personal data stored in the Library's computer system for the purpose of performing library work. We will not disclose any personal data we collect from you to any other party except where required by law or to fulfill an individual user's service request. The Library does not sell or lease users' personal information to companies, universities, or individuals.

Enforcement and Redress

Our library will not share data on individuals with third parties unless required by law. There are certain provisions of the [USA PATRIOT Act](#) which can allow law enforcement officials to request information without your knowledge. Library users who have questions, concerns, or complaints about the library's handling of their privacy and confidentiality rights should file written comments with the Director of the Instructional Resources. We will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

We authorize only the Director of Instructional Resources, our Vice President of Academic Affairs, and our Director of Campus Security to receive or comply with requests from law enforcement officers; we confer with our legal counsel before determining the proper response. We will not make library records available to any agency of state, federal, or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form.

This policy derives from the American Library Association web site, entitled "[Guidelines for Developing a Library Privacy Policy.](#)"

Appendix D. Library Privacy Policy Statement (Final Policy Recommendation Approved by MnSCU)

It is the policy of the Livingston Lord Library of Minnesota State University Moorhead to respect the privacy of its patrons to the extent permitted by law. The Library's privacy practices are consistent with applicable state and federal privacy laws including, but not limited to, the Minnesota Government Data Practices Act ([MGDPA](#), Minnesota Statutes Chapter 13) and the Family Educational Rights and Privacy Act ([FERPA](#), 20 U.S.C. 1232g), as well as professional standards of the [American Library Association](#). Minnesota State University Moorhead is part of the Minnesota State College and University System and is subject to its Board Policies and Procedures, which may be found at: <http://www.mnscu.edu/board/policy/index.html>

The following information maintained by the Library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order, or as otherwise required or permitted by law:

1. Data that link a Library patron's name with materials requested or borrowed by the patron or that link a patron's name with a specific subject about which the patron has requested information or materials; or
2. Data in applications for borrower cards, other than the name of the borrower.

Additional information about your data rights as an individual and the university's responsibilities concerning the handling of private data may be found as the following website: [MSU Moorhead Campus-Wide Guidelines For Computer And System Use: Responsible Behavior And The Electronic Media Data Privacy And Security](#)

Retention Policies

Information we may gather and retain about current and valid library users include the following:

- User Registration Information is maintained indefinitely in the current Library catalog software. In the future, some User Information may automatically delete when the system is upgraded to newer software versions.
- Circulation Information is not kept in the form of a permanent ongoing record of borrowing for any individual. Once materials are returned, that record is deleted. However, the Library system's back-up files may retain borrowing information for up to 60 days after an item is returned. Records where fines have been incurred are maintained indefinitely.
- Electronic Access Information is not made available to any other entity outside the Library except as required by law. The Library maintains statistics only of database usage statistics.
- Information Required to Provide Library Services such as consultation services in the form of reference or research consultation will only be shared outside the Library with third parties under certain circumstances as required or permitted by law. InterLibrary Loan service necessitates the sharing of patron information between libraries, but will only be disclosed during these transactions if necessary to conduct Library business.

Online Privacy Practices

The policy of the Livingston Lord Library at Minnesota State University Moorhead is to respect the privacy of all web site visitors to the extent permitted by law. This online privacy statement is intended to inform you of the ways in which this web site collects information, the uses to which that information will be put, and the ways in which we will protect any information you choose to provide us.

Data Integrity : The data we collect and maintain at the library must be accurate and secure. We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to your own personally identifiable data; updating data whenever possible; destroying untimely data.

Data Retention : We protect personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services.

Tracking Users : The system removes links between patron records and materials borrowed when items are returned and records are deleted as soon as the original purpose for data collection has been satisfied, with the exception of fines. Currently, the system default for all MnPALS Libraries is 60 days. We permit in-house access to information in all formats without creating a data trail. We do not ask Library visitors or Web site users to identify themselves or reveal any personal information unless they are borrowing materials, requesting special services, registering for programs or classes, or making remote use from outside the Library of those portions of the Library's Web site restricted to registered borrowers under license agreements or other special arrangements. We discourage users from choosing passwords or PINs that could reveal their identity, including social security numbers. We regularly remove cookies, Web history, cached files, or other computer and Internet use records and other software code that is placed on our computers or networks. The computers in the Library currently operate under a software program which reverts the hard drive back to its original state after two hours of inactivity. At a minimum, this process is done daily.

Third Party Security : We strive to ensure that our Library's contracts, licenses, and offsite computer service arrangements reflect our policies and legal obligations concerning user privacy and confidentiality. When connecting to licensed databases outside the Library, we release only information authenticating users as "members of our community."

Cookies : Users of networked computers will need to enable cookies in order to access a number of resources available through the Library. A cookie is a small file sent to the browser by a Web site each time that site is visited. Cookies are stored on the user's computer and can potentially transmit personal information. Cookies are often used to remember information about preferences and pages visited. You can refuse to accept cookies, can disable cookies, and remove cookies from your hard drive. Our Library servers use cookies solely to verify that a person is an authorized user in order to allow access to licensed library resources and to customize Web pages to that user's specification. Cookies sent by our Library servers will disappear when the user's computer browser is closed. We will not share cookies information with external third parties.

Security Measures : Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

Staff access to personal data : We permit only authorized Library staff with assigned confidential passwords to access personal data stored in the Library's computer system for the purpose of performing Library work. We will not disclose any personal data we collect from you to any other party except where required by law or to fulfill an individual user's service request. The Library does not sell or lease users' personal information to companies, universities, or individuals.

MSUM web sites provide links to other World Wide Web sites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by the University's online privacy policy; they may have their own policies or none at all. Often you can tell you are leaving a University web site by noting the URL of the destination site.

Minn. Stat. 13.15 provides that electronic access data may be disseminated: (1) to the commissioner for the purpose of evaluating electronic government services; (2) to another government entity to prevent unlawful intrusions into government electronic systems; or (3) as otherwise provided by law.

Enforcement and Redress

Our Library will not share data on individuals with third parties, including law enforcement, unless required or permitted by law. There are certain provisions of the USA PATRIOT Act which can allow law enforcement officials to request information without your knowledge. Library users who have questions, concerns, or complaints about the Library's handling of their privacy and confidentiality rights should file written comments with the Director of the Instructional Resources. We will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

We authorize only the Director of Instructional Resources, our Vice President of Academic Affairs, and our Director of Campus Security to receive or comply with requests from law enforcement officers; we confer with our legal counsel before determining the proper response. In most cases, we will not make library records available to any agency of state, federal, or local government unless a subpoena, warrant, court order or other investigatory document is issued by a court of competent jurisdiction that shows good cause and is in proper form.