WORKING PAPER: IS PRIVACY WORKING? PLANNNING FOR STRONGER PRIVACY MEASURES THAN SECURITY THROUGH OBSCURITY by Mary Minow and Paul Neuhaus

WORK IN PROGRESS – Please do not cite without permission

American Library Association Office of Information Technology preconference
"Digital Reference and Legal Issues," on June 23, 2005

WORKING PAPER: IS PRIVACY WORKING? PLANNNING FOR STRONGER PRIVACY MEASURES THAN SECURITY THROUGH OBSCURITY IN LIBRARY VIRTUAL REFERENCE SERVICES

by Mary Minow and Paul Neuhaus
Presented June 23, 2005, rev. Sept. 15, 2005

I. Introduction –Samantha's Reference Questions Seen Cross-Country

Poor Samantha. She is quietly considering leaving her husband, and wants to get reliable information about divorce, housing, and related issues. But that's not the dilemma. The issue is whether her husband, his attorney, her nosy neighbor hacker, her librarian cousin in another state, or even law enforcement will discover her inquiries.

The reference librarian helping Samantha is committed to maintaining Samantha's privacy. The problem at hand is that her chat with the librarian, which once would have quickly dissipated into the air, is now recorded and preserved. Once recorded, records can live on and on and on…vulnerable to a host of viewers from collaborative partners, to vendors to hackers. Further, virtual reference records are subject to civil and criminal subpoenas, as well as search warrants and PATRIOT Act orders.

While privacy problems connected with virtual reference have not been severe to date, virtual reference collaboratives should not rely on privacy through obscurity. It is only a matter of time until data breaches are reported or requests are made by law enforcement or others for user records.

Policies and procedures should ensure that privacy measures minimize harmful data breaches and to prepare for the inevitable future requests for virtual reference user records.

II. Collaborative Virtual Reference Policies and Procedures Should be Consistent with the Fair Information Practices as Described in the American Library Association Model Privacy Policy

A. Need to protect virtual library user's privacy

Library ethics strongly affirm the importance of patron privacy as a core value.[1] In implementing virtual reference, this long held value must be undeniably incorporated. While it is possible to *gain* additional user privacy by virtue of faceless interactions, it is especially possible to *diminish* privacy due to an automated collection of IP addresses, an active collection of names and email addresses and keystroke by keystroke collection and maintenance of reference transcripts – none of which were routinely created nor kept in the analog library reference world.

Before digital reference, most patron reference interactions left no records. In the digital realm, transcripts of questions and answers are typically maintained, registration data gathered, IP addresses collected, etc. In addition, if a digital reference service is hosted by a vendor or the vendor stores the transcripts, records are often outside the control of the library. These significant differences in reference methods significantly raise privacy concerns. These concerns may continue to grow as new technologies come on the market and are utilized for reference services.

As one of the authors has previously written in his article "Privacy & Confidentiality in Digital Reference," gives a detailed discussion of privacy issues raised by the creation of virtual reference records. He writes that the need to protect library patrons' privacy appears to be self-evident, but is not necessarily so.[2]

Marc Rotenberg, executive director of the Electronic Privacy Information Center (EPIC), sums up the importance of privacy in a library:

> Libraries to me have always seemed to sit at the very core of information rights in a democratic society. I can think of no place where the twin interests of public access to public information and respect for privacy of personal information is more greatly respected than in the library.
>
> Let's think about this for a moment. A person enters a library. They literally have at their fingertips access to all the information available in that institution and connected and linked and networked to other institutions in the community, across the country, and around the world. It is still the case that in the vast majority of institutions it is possible for people to get access to information without having to disclose their identity. There may be some qualifications; you may need to be a member of an institution to get access. There may even be some records created in an electronic environment that enable access through new search systems.
>
> But as a general matter this is how we view the library, an institution that provides access to information and, simultaneously, provides extraordinary respect for the freedom of the individual to protect his or her identity if they so wish.[3]

Library privacy discussions have heated up in recent months, as Congressional hearings have been held to renew Section 215 ("the library records provision") of the PATRIOT Act.[4] Combined with escalating reports of data security breaches at university and government sites[5] a detailed look at virtual reference privacy is imperative.

In May 2005, the American Library Association (ALA) issued a revision of its Privacy Tool Kit, offering libraries a solid background on library user privacy as a core value of librarianship.[6] In sum, one cannot truly exercise the right to read if the consequences could damage one's reputation or even worse, result in criminal penalties. Additionally, the Toolkit gives guidelines to draft privacy policies, a model privacy policy (Appendix B), how to conduct a privacy audit, and more.

When a library joins a collaborative, it is critical that the collaborative's privacy policy and practice is consistent with the library's own privacy policy. This paper suggests a model privacy policy and procedures at the collaborative level, consistent with the ALA Model Privacy Policy, the basis of many individual library policies.

Patrons should have the ability to research anonymously. They should be able to perform the electronic equivalent of talking to an information professional and receive quality information without leaving digital tracks unless they affirmatively wish to do so.[7]

1. Virtual library user anonymity

User Anonymity is the highest form of user privacy. The library has no records to turn over. In traditional library reference interviews, personally identifiable information (PII) of users is not taken unless a follow-up response by the library is required. Users who ask questions by telephone can enjoy even greater anonymity, eliminating face-to-face contact. Call-ins by pay phone can be virtually untraceable.

Sociologist Gary T. Marx enunciates common contexts in which anonymity and identifiability are viewed as socially desirable. He classifies 15 rationales in support of full or partial anonymity, including one particularly relevant to the reference interview:

> 4. to encourage reporting, information seeking, communicating, sharing and self-help for conditions that are stigmatizing and/or which can put the person at a strategic disadvantage or are simply very personal.[8]

Included in his examples are "self-help requests and discussion and support groups for alcohol, drug, and family abuse, sexual identity, mental and physical illness," and "communicating about personal problems and issues with technologically distanced (and presumably safer) strangers."[9]

2. Virtual library user confidentiality

In contrast, **user confidentiality**, in which the library has information about a user but does not disclose it, forms the basis of most state library confidentiality laws. Traditional library circulation services create user records in most cases, honor checkouts being a notable exception.[10] Library card numbers are linked to library books or other materials, for at least as long as the items are borrowed by the user. In many cases, although the link is broken when the material is returned, these records linger on through library backup systems.

Although libraries have long experience with keeping user records confidential, the sheer number of players with access to virtual reference records requires additional care. Referrals are made to librarians outside the library, vendors may have access to the records, and the transmission of records increases the risk of hackers obtaining access. Moreover, in an age of increasing surveillance, interception by the government is in the realm of possibility.

Libraries should ensure by contract that satisfactory privacy policies and procedures are in place at the collaborative level, with vendors as agreeing parties.

Since federal and state law do a poor job at protecting a library's virtual reference records, libraries need to carefully adopt library policies and procedures to ensure that they maximize privacy.

B. Privacy law models

According to the Electronic Privacy Information Center, efforts to protect privacy generally fall into one or more of the following models:

> Comprehensive laws are general laws that govern the collection, use, and dissemination of personal information. Typically an oversight body ensures compliance. The European Union is an example of this type of approach to privacy protection. A variant of this model is the co-regulatory model in which an industry develops rules and enforces them with a privacy agency. Australia and Canada are two countries that use this variant.
>
> Sectoral laws represent a second model. These laws focus upon particular industries or sectors of society. Sectoral laws are often used to complement comprehensive legislation by providing more specific protections. One drawback to this method is that new legislation is required as new technologies emerge. Hence, legal protections often lag. Enforcement of sectoral laws is achieved through a variety of mechanisms. The sectoral law model is used in the United States.
>
> A third model is self-regulation. Companies or industries establish codes of practice and self-police. This model often provides weak protection and little enforcement. Singapore and the United States are two countries that utilize this model.
>
> The fourth model is technologies of privacy that are chosen by individual users. These include encryption, anonymous remailers, proxy servers, etc.[11]

Virtual reference records are subject to sectoral privacy laws in the U.S. As a result, the law is somewhat difficult to piece together. Traditional library records are addressed by state library confidentiality statutes.

Yet virtual reference records cross state lines, and collaborative arrangements can include not only a mix of public and private libraries, but even a mix of local, state and federal libraries.

Moreover, the law splinters privacy protection based on whether the library is federal, state, local or private. In that model, a collaborative virtual reference privacy policy must cover a broad range of libraries. It is not practicable to present a user (or an administrator for that matter) with multiple privacy policies depending on whether the record is local (like some email reference) or part of a collaborative. This paper recommends that privacy policies be set at the collaborative level, and that they encompass at least the level of privacy as mandated by the strictest law that governs any one of its members or potential members.

C. International law and virtual reference records

Virtual reference collaboratives can cross international boundaries. Different nations use entirely different regulatory schemes to administer electronic communications. For example, Voice over IP (VOIP) is subject to a new regulatory framework adopted by the European Commission in 2002 that includes a Privacy Directive, while the United States regulates VOIP under the Telecommunications Act of 1996 using outdated categories of "information services" and "telecommunication services,"

Canada regulates privacy at both the federal and provincial levels. The 1982 federal Privacy Act regulates personal information held by federal public agencies, which was drafted in part based on the Organization for Economic Cooperation and Development (OECD)'s 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Nations that place restrictions on the transborder flow of personal data ensure that any personal information relating to its citizens is protected by law when it is exported to or processed in outside countries. Carefully drawn contracts are necessary to satisfy international requirements.[12]

Federal law and virtual reference records

The U.S. Constitution probably does not protect users' library records of any type. Although there is no direct case law on constitutional privacy and library records, the Supreme Court has developed a doctrine in which the voluntary sharing of one's records with a third party deeply reduces one's expectation of privacy.[13]

Although Congress has considered broad bills to codify fair information practice requirements, only narrow applications have passed to date.[14]

Federal librarians are subject to laws such as the Privacy Act of 1974, which allows citizens to gain access to their own records, maintained by federal agencies (including federal libraries).[15] Executive memoranda require federal agencies to ensure their information practices adhere to the Act. At least one memo states that "persistent" cookies which remain on a user's computer for varying lengths of time are not allowed unless four specific conditions are met. "Session" cookies, which expire when the user exits the browser, are permitted.[16] Federal librarians have had training sessions on the E-Government Act of 2002 which requires certain fair information practices for federal agency websites.[17] The Office of Management and Budget provides specific guidance to agencies implementing the Act in Memorandum M-03-22.[18] Privacy impact assessments must be conducted by federal agencies when they develop or procure projects that collect, maintain or disseminate PII. The Act also requires agencies to write their privacy policies in a standardized machine readable format, in order to automatically communicate to users whether the site privacy practices match their personal privacy preferences using P3P.[19] If federal agency libraries are part of a collaborative reference service, these laws and regulations must be taken into account.

Virtually all libraries are subject to the Electronic Communications Privacy Act (ECPA) which regulates "remote computing services," defined broadly enough to encompass libraries that provide services to the public by means of an electronic communication system.[20] The ECPA, which governs access, use, disclosure and interception of electronic communications, likely applies to both the live transmission of virtual reference and to the records created.

The ECPA authorizes government administrative subpoenas to compel disclosure of transactional records such as user names, addresses and length of service. It authorizes disclosure of content by court order. Of special interest to virtual reference librarians, perhaps, is its provision that allows providers to divulge the contents of a communication to a federal, state or local government entity if the provider believes, in good faith that an ***emergency involving danger of death or serious physical injury*** requires disclosure without delay.[21]

The Family Educational Rights and Privacy Act (FERPA)[22] is often seen by librarians as an additional layer of protection of library records held by schools and universities that receive federal funding. However, the Act does not explicitly cover library records but covers "education records," defined as school records with information directly related to a student. Directory information (including, among other items, name, address, phone number) are not protected under the Act.

D. State law and virtual reference records

Although most discussions of library privacy centers on state laws written specifically to protect library records, one should also look for newer state laws governing the electronic collection of personal information.

For example, California state agencies have had specific requirements with regard to handling PII since 2001 under California Government Code §11015.5 (shown in full in Appendix). State agencies must give **notice** to users of the existence of information gathering, the type of personal information collected, and they must give users an **option** to have PII discarded. The agencies must not distribute the PII to third parties without user **permission**, and user PII is specifically exempted from the state public records act. Users must be given a contact person to **enforce** the law. Exceptions are made to investigate Penal Code violations and other authorized exceptions under the state information practices act.

Are virtual reference records covered by the state library confidentiality laws? These statutes vary considerably from state to state with regard to how records are defined, and what conditions permit disclosure. The definition of records is frequently too narrow to protect virtual reference records. A draft model state law, updated to more broadly define today's range of library records, is in the Appendix.

In twenty-one states, library records are exempted from state open records or freedom of information act (FOIA) laws. Thirty three states plus the District of Columbia have specific laws to provide protection of library records. Five states use a combination of both designated library confidentiality statutes and exceptions to state FOIA laws. Hawaii and Kentucky do not have laws protecting the confidentiality of library records but they do have Attorneys General opinions supporting privacy of some library records.

Table 1: States that Protect or Do Not Protect Virtual Reference Records in Library Confidentiality Statutes

Probably Protect	**Maybe Protect**	**Probably Do Not Protect**
Alabama	Delaware	Alaska
Arizona	District of Columbia	California
Arkansas	Georgia	Connecticut
Colorado	Idaho	Florida
Indiana	Kansas	Hawaii
Iowa	Michigan	Illinois
Maryland	Missouri	Kentucky
Massachusetts	Montana	Louisiana
Minnesota	New York	Maine
Nebraska	Oregon	Mississippi
New Hampshire	Washington	Nevada

North Carolina		New Jersey
North Dakota		New Mexico
Ohio		Oklahoma
South Carolina		Pennsylvania
South Dakota		Rhode Island
Tennessee		Virginia
Texas		West Virginia
Utah		Wyoming
Vermont		
Wisconsin		

Libraries should carefully read the current version of their state law in consultation with an attorney.[23] Further detail is in the Appendix.

E. Children's virtual reference records and the law

1. Federal law

Recognizing a special vulnerability in children under the age of 13, federal law requires certain commercial website owners to follow some fair information practices. The Children's Online Protection Privacy Act (COPPA)[24] requires commercial sites that are directed to children under 13 or that knowingly collect information from them to give ***notice –*** that is, parents must be informed of the site's information practices. Commercial sites must also obtain verifiable parental ***consent*** before collecting, using, or disclosing personal information from children.

Although COPPA does not apply to noncommercial sites, it sets some expectations by parents as to what best practices websites should use when asking for their children's information. The American Library Association's discussion of libraries and COPPA can be found on its website.[25]

Federal law may lessen protection to children's records under the Family Educational Rights and Privacy Act (FERPA), by allowing parental access. Although the language is not clear, and it has not been tested in court, if indeed FERPA applies to library records, then parents may have a right under FERPA to their children's records. It may also be argued that "education records" do not include library records. If this interpretation prevails, it would strip the layer of protection from the records discussed above with regard to users over 18.[26]

2. State law

State library confidentiality laws sometimes give less protection to children's records than to adults' records. In each state that makes such a provision, this additional disclosure is essentially limited to parents or guardians. The Appendix gives more detail.

F. Discussion on drafting a virtual reference collaborative privacy policy using fair information practices

The authors of this paper invite rigorous discussion and mark-up of the draft policy proposed in Section V both during the American Library Association Office of Information Technology preconference on "Digital Reference and Legal Issues," on June 23, 2005 and by email.

The draft policy aims to build on the foundations already developed by the ALA Model Privacy Policy, the ALA Reference and User Services Association Machine-Assisted Reference Section (MARS) Ad Hoc Committee's Guidelines for Implementing and Maintaining Virtual Reference Services, a current collaborative's Privacy Statement and Paul Neuhaus' privacy recommendations summarized in his Digital

Reference and Privacy website, drawn from article, "Privacy & Confidentiality in Digital Reference." Reference & User Services Quarterly 43, no.1 (Fall 2003).
Additionally, the draft policy aims to consider legal requirements established for California state agencies as set forth in California Government Code §11015.5.

Excerpts from these sources are reprinted in the Appendix.

The ALA Model Privacy Policy articulates five fair information practice principles as an organizing mechanism: **Notice** and Openness, **Choice** and Consent, **Access** by Users, **Security** and Data Integrity, and **Enforcement** and Redress. An international consensus has emerged for elements of privacy that relate to the collection, maintenance, use, disclosure, and processing of personal information. In the last twenty years, fair information practices have become an international standard for privacy. In recent years, virtually all privacy laws enacted around the world are an implementation of some variation of fair information practices.[27]

This section aims to apply those principles to the virtual reference environment, as well as to raise some of the thornier issues for discussion. Because of the complex arrangements inherent in nationwide and international collaboratives, many of the issues require expanded discussion of the privacy principles that guide an individual library. Further, the devil is in the details; Section III delves more deeply into specific features in current technology, such as encryption, server storage locations etc … offering a draft roadmap for collaboratives to perform their own privacy audits.

1. Preamble: Limitations on collection, purpose and use

What records are necessary to collect in the first place? The ALA model privacy policy discusses minimizing the collection of user records as part of its discussion on Notice and Openness: "In all cases we avoid creating unnecessary records..."

Unlike library circulation and registration records which are necessary to run a library, virtual reference records are created as a byproduct of digitizing a service that, in the analog world, did not create records. A virtual reference policy necessarily must carefully look at the ***initial creation*** of records in the first place. Once the records are created, it should promise to limit the use of those records to the primary purpose – answering user reference questions, absent user consent, or as required by law.

Recommendation: Include preamble on limitations of collection, purpose and use.

2. **Notice** & openness

While notice is important, it must be recognized that it is entirely possible to give users notice of a policy without actually protecting their privacy. Often notice seems to operate as a waiver or disclaimer. It is much better to simply build-in privacy. As Marc Rotenberg write, "Privacy should be under the hood, not on the dashboard."[28]

Many privacy policies reserve the right to make changes at any time. Although this is desirable from an institutional standpoint, such a reservation must be written carefully. Significant changes in the use of PII will only be made prospectively, and not for previously collected information.

> "It's simple – if you collect information and promise not to share, you can't share unless the consumer agrees … You can change the rules but not after the game has been played."[29]
>
> - Howard Beales, Director of the Federal Trade Commission Bureau of Consumer Protection, in reference to an FTC consent order that bars Gateway Learning Corp. from applying material changes to its privacy policy retroactively

In the spirit of notice, it's also recommended that libraries and collaboratives prominently display notices when material changes are made. Links to the library's own privacy policy should be placed on the page that opens to the virtual reference service.

Recommendations: Reserve the right to change the privacy policy *prospectively* only. Display a link to the library's own privacy policy on every page, especially to pages that collect PII such as virtual reference login pages.

Further Discussion: How can a library reconcile a collaborative's privacy policy with its own? What problems might ensue if the collaborative's privacy policy is stronger than the library's? What if it is weaker?

3. **Choice** & consent

While choice and consent may give users options as to how their PII is collected and used, privacy critics caution against an over reliance on the choice and consent principles. "Fair information practices call for personal information to be used in clearly defined ways identified in advance. The notion of *choice* is a distortion because it allows any use of data as long as the data subject has been offered some opportunity, no matter how difficult or remote, to object."[30]

Library collaboratives should offer true choice and consent whenever possible. A choice to *not use the service* is not optimal, although if PII is essential, at a minimum the user should be directed to alternative means of reference service such as telephone and walk-in service.

Offering a choice to remain anonymous is the best option, and should be made available whenever a library is able to serve users outside its own defined community, whether tax-based or privately funded. Due to the collaborative nature of virtual reference, jurisdictional lines are starting to blur, strengthening an argument that some leeway can be given to allow outsiders in, since they can come in through referrals in any event.

An anonymous choice is more difficult to construct when proprietary databases are used, since vendors need to ensure that only authorized users are allowed. See Section IV for further discussion.

Choice and consent presents a challenge for anyone wanting to use transcripts for research purposes. Must each patron be notified and give explicit consent for records to be used? The answer may depend upon how much PII is collected and an assessment of the potential harm to patrons. Such assessments must abide by the Federal Policy for the Protection of Human Subjects (45 CFR 46). Many colleges and universities have Institutional Review Boards (IRBs) that attempt to apply the Human Subjects policy to specific research requests. Approval by such bodies is a necessity before researchers can begin working with the records.

Recommendation: Offer anonymity as a choice whenever possible.

Further Discussion: For libraries or collaboratives that are not able to offer an anonymous choice, is "authentication without identification" viable? Should consent be required to use PII for promotion, research, or any other purposes beyond the primary purpose of conducting virtual reference?

4. **Access** by users

This is not a difficult issue, in that users readily see their own reference transactions as they are created. Further, they are emailed copies of the transcripts if they provide an email address. Anonymous users (for systems that offer this service) may secure a copy of their transactions by using a URL provided by the service.

Further Discussion: Should users be offered a copy of their clickstream data (IP address, browser etc.)?

5. **Security** and data integrity

Unlike book circulation records, virtual reference records are often transmitted in clear text across the Internet. Section III discusses encryption, etc.

6. **Enforcement** and redress

Perhaps the thorniest issue that virtual reference raises is the *multiplicity of partners*, many of whom have some access to some of the data, at least some of the time. In that the parties have varying legal obligations with regard to user confidentiality, it is recommended that all partners agree by contract to uphold the virtual reference collaborative's privacy policy.

Bargaining power with vendors here is especially important. Vendors that have a majority of clients who are not concerned with privacy issues will likely be more difficult to negotiate with. If a library simply *uses instant messenger software* commonly available on the Internet, it may be impossible to satisfy privacy concerns.

1. Draft contract clause

> All PARTIES are committed to protecting user privacy online. All PARTIES agree to adhere to the [Collaborative Virtual Reference] Privacy Policy.

The California Digital Library (CDL), includes confidentiality in its checklist of license agreement points:

> **Confidentiality:** The confidentiality of individual users must be maintained. User data should not be reused or sold to third parties without permission. The CDL requires that vendors comply with the UC privacy policy and the ICOLC privacy guidelines for electronic resource vendors.[31]

2. ICOLC Guidelines

Many content vendors have signed on to the International Coalition of Library Consortia (ICOLC) Guidelines, promising not to disclose PII, although reserving the right to send information such as an IP address or user ID to a third party that needs to ensure that only authorized users have access to their content.

Here is an excerpt from the California Digital Library's Technical Requirements for Database Vendors, requiring adherence to ICOLC Privacy Guidelines:

> 14. Privacy:
> Confidentiality of individual users must be maintained. User data should not be reused or sold to third parties without permission. At minimum, the vendor's policy should conform to the ICOLC Privacy Guidelines for Electronic Resources Vendors. Elements that should be addressed in the vendor's privacy policy include:
>
> - who collects user information and who has access to it
> - what information is collected
> - why the information is collected
> - the duration for which the information is retained
> - when the policy was devised and when it might be revised
> - where the privacy policy originated and how to contact its originators
>
> Please provide a copy of your current privacy policy.
>
> California Digital Library, Technical Requirements for Database Vendors, June 5, 2001, Latest revision October 28, 2004[32]

Here is an example of ABC-CLIO's privacy policy stating that it adheres to the ICOLC Guidelines:

> ABC-CLIO supports the ICOLC Privacy Guidelines for Electronic Resource Vendors (http://www.library.yale.edu/consortia/2002privacyguidelines.html). ABC-CLIO is committed to protecting user privacy online. We believe that strong electronic privacy is crucial for the ongoing success of the Internet. We also believe it is critical for us to adhere to the American Library Association's Code of Ethics. We pledge to give you as much control as possible over your personal information. We will not disclose individually-identifiable information about you to any third party without your consent. We will not sell of [sic] rent any personally identifiable information to a third party. This information will only be used by ABC-CLIO internally or to send you information you have requested. Click here to view the entire ABC-CLIO privacy policy. [33]

Further Discussion: What privacy clauses (if any) do parties agree to presently? Can the ICOLC guidelines be incorporated or adapted to serve the partners, including vendors, in collaborative virtual reference services? What penalties should be applied in the case of a breach of privacy?

III. Virtual Reference Privacy Audits – Technical Information

A. Privacy and technical features in virtual reference

The following are important issues when conducting a privacy audit of a digital reference service. This list is not intended to be exhaustive. The table at the end of this section illustrates how selected vendors address these issues.

1. What PII is gathered

A wide range of PII can be gathered from digital reference records. There are two categories of PII. The first category consists of information that a user intentionally provides, such as name, address, email address, and library card number. The second category consists of ***clickstream data*** that automatically accompanies visitors to any website: their IP address or hostname of the user's computer, browser type, operating system, time of arrival and departure, and referring URL.

A privacy audit should begin with three questions: (1) What information is absolutely essential for the operation of this service?, (2) What information would be useful to know but is not essential?, and (3) Is there a way to block unwanted information, particularly the user's IP address, which can often lead an investigator to the user? The guiding principle ought to be to only collect a minimum of essential information.

2. Anonymity

The opportunity for patrons to remain anonymous varies considerably from vendor to vendor and from collaborative service to collaborative service. The strongest anonymity option allows a user to remain anonymous to register, including blocking the user's IP address.

Sample information automatically collected when using anonymous option in 24/7 Reference via Santa Clara County Library portal:

Name: anonymous Email Address: anonymous Library: anonymous City: anonymous Question: Are there any articles written about privacy and online database searching - that is, when someone searches a library database from home, and has to enter their card number, is the library or the database vendor able to see what the user was searching? Virtual Category: SCLARACOUNTY Browser: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Tablet PC 1.7; .NET CLR 1.0.3705; .NET CLR 1.1.4322) IP address: anonymous Connection: Hi-speed Firewall: Yes

A second option does not offer an explicit anonymity option, but allows users access without registration, leaving only the digital clickstream data such as IP address.

A third alternative allows the user to identify herself when accessing the service but can honor a request to remove the users PII as entered at the user registration screen.

Fourthly, some services require minimal, nonidentifiable information such as an email (and any name) or a zip code. A user concerned with anonymity may use a hotmail-type account or make up a zip code. Finally, some services require authentication, such as a user barcode and PIN. This option precludes anonymity and is used when an institution must limit its services to its own user community.

In all of these alternatives, identifying information disclosed in the context of the chat interaction itself will remain. Users who affirmatively request that their PII be stripped should be warned about this, and given the option to remove the entire transaction from the service's servers, and any copies residing elsewhere.

3. Encryption

The use of encryption varies among VR vendors. Vendors that serve both library and commercial clients (e.g., banks) appear more likely to offer encryption due to the sensitive nature of some transactions. When encryption is offered, typically only registration or other PII data is encrypted. The remainder of the VR transaction is left unencrypted. Encrypted pages require greater server resources though there is some movement toward encrypting all web pages associated with a site as technology improves.

4. Storage Site and Partner Access to Transcripts

This is an important question since information stored on a third party site (vendor) likely has less legal protection than information stored on a library's server. In a collaborative arrangement, is the information stored on the vendor's site, a library member's site, or at each library? A related issue arises when a government library is part of the collaborative effort. If a public library is a consortia member, the data may reside outside the library's control, and even an individual library may use a municipal server rather than its own.

This is an important technical point that must be addressed by contract arrangements to ensure that all parties agree to uphold the collaborative's privacy policy.

This question can also have an international dimension. By law, libraries and archives that are part of the Canadian federal government must maintain their data on Canadian servers. This can present a challenge when the library or archive is part of an international collaborative effort. There may also be reluctance by Canadian libraries to use VR services headquartered in the United States if the records are stored on the vendor's server. Such records would fall within the jurisdiction of the PATRIOT Act.

5. Retention of Digital Reference Records

This issue applies equally to VR transactions, email queries, and web form questions. Policies vary considerably by library, thus collaborative partners must take the lead in setting policies. When a deletion schedule is decided upon, a key component is to ensure that all backup copies located on servers, tapes, or other media are included. In addition, government and public libraries may be subject to government retention schedules and guidelines. At the present time, no known government retention schedules address virtual reference records.

6. Staff Logins

Many libraries require staff to authenticate to the organization's computer system to use the organization's online resources. If the librarian subsequently staffs the VR service, this login information is not transferred to the vendor. However, if a librarian logs in to the VR service (e.g., as a means to personalize the service or the virtual reference software requires individual staff logins), this information would then become part of the record.

7. Cookies

Cookies are software code sometimes used by vendors to facilitate a VR interaction. Some cookies store records from previous transactions so the librarian can better follow the thread if the patron's question is a follow-up. Cookies may also be used by vendors to enable certain features such as co-browsing. Cookies should never be used to transmit personal information about the user to the vendor.

8. KnowledgeBases

KnowledgeBases are collections of digital reference records created either automatically or manually from digital reference interactions. If a knowledgebase is intended for internal use only, PII can be retained in the records though only staff with a "need to know" should have access. If a KnowledgeBase is intended for publication, it is imperative that all PII be stripped from the record, including any PII found in the body of the interaction. Stripping clickstream and registration data can be automated but each transcript must be perused individually to ensure the removal of all PII within the body of the transcript.

9. Statistical Summaries and Other Reports:

Two types of reports fall within this category and are often mentioned as allowable under state laws regarding library records. Internal reports that are considered the "business of the library" can include PII data. As with internal KnowledgeBases, these should be available only on a "need to know" basis. The second category encompasses published reports in which all identifying information is stripped from the record before publication. Canadian privacy law makes a distinction that may be important here, namely, that the individual need not be identified, just identifiable. These report principles are applicable to all partners in the virtual reference collaboration.

B. Vendor options currently available

Table 2 illustrates how some vendors and libraries handle these issues for live reference services.

Table 2

Virtual Reference Software and Privacy Features

This table summarizes the privacy features of various software products. A more detailed description of each product follows the chart.

Product	Encryption Level	Registration or Login Required	Identifying Information Collected	Anonymity Options	Storage Site for Transcripts	Retention Period for Transcripts	Deleted Records Retrievable from Back-Up Systems?	Court Orders for Transcripts	Wiretaps, Trap & Trace Devices?
24/7 Reference	No encryption	Discretion of library	Discretion of library	Anonymity	Vendor or library	One year	Yes, but "hideously difficult"	Never	Never
ChatSpace	No encryption	Optional	Discretion of library	None	Vendor or library	Discretion of library	Yes	Never#	Never
ConferenceRoom	128 Bit	Optional	Discretion of library	None	Vendor or library	Discretion of library	No	No*	Never **
Desktop Streaming	128 Bit	--	E-mail, IP address	None	Vendor	Maximum of 6 months	Yes	Never	N/A
LiveAssistance	Only in advanced package	Yes	Discretion of library	None	Vendor or library	Discretion of library	No	Never	Never
LivePerson	128 Bit	Discretion of library	Discretion of library	None	Vendor	Discretion of library	Yes	Never	N/A
OnDemand (Convey), hosted version	128 Bit	Yes	Name, e-mail, IP address	None	Vendor	Discretion of library	No	Never	N/A
OnDemand (Convey), licensed version	128 Bit	Yes	Name, e-mail, IP address	None	Library	Discretion of library	Unknown	Never	N/A
Virtual Reference Toolkit	Unknown	Optional	Discretion of library	Anonymity; opt out	Vendor or library	Discretion of library	No	Never	N/A

From Paul Neuhaus, Virtual Reference Software and Privacy Features (web page). More detail at http://www.library.cmu.edu/People/neuhaus/software.html.[34]

IV. Connecting to Broader Issues, Parallel Issues, and Subsidiary Issues

Linda Arret, Project Coordinator, Digital Reference Legal Issues has raised a number of issues for exploration over the years. This section is intended to shape some discussion issues, within the context of the legal framework in Section II or supplied directly here.

These issues would benefit from the shared discussion, expertise and opinions of the participants at the OITP digital reference legal issues preconference.

A. Children, COPPA and the Library Bill of Rights

Is it possible to comply with both the spirit of COPPA (protecting young children from giving out their PII) and with the Library Bill of Rights which states that a person's right to use a library should not be denied or abridged because of age?

Would an anonymous option help to solve this dilemna, since children would not be required to provide PII?

B. Staff Privacy

Is it appropriate to protect staff privacy, and if so, to what extent? Public institutions are subject to state open records laws and do not have the same discretion as private institutions concerning staff privacy. Should staff privacy be addressed in a collaborative's virtual reference policy? If so, how would it handle the distinct difference between librarians in public institutions versus librarians in private institutions?

An illustration of a public library unable to provide privacy to its staff can be found in the Tacoma Public Library case. In that case, a union representative asked the library for employees' names, salaries, vacation, benefits and pension information. This information was organized in city records by employee name and identification number. The Library argued that disclosure of an employee's name coupled with his or her identification number would permit access to other exempt personal information, such as the employee's social security number, home address, and telephone number, by anyone logging onto a City of Tacoma computer. A Washington state appellate court ordered the release of the employee names, salaries and benefits but did allow redaction of the identification numbers.[35]

C. PATRIOT Act and other legal inquiries that libraries and vendors may be susceptible to (e.g. wiretaps, court orders, subpoenas) and responses (e.g. quashing subpoenas)

Many privacy policies do not mention that despite the best intentions to keep PII confidential, the reality is that the sessions and the records they create are susceptible to wiretaps, court orders, subpoenas and other legal process. The PATRIOT Act has galvanized many in the library community to prepare for law enforcement and other requests for patron records. Much has been written on how to respond with regard to circulation and Internet use records, and the same analysis would apply to virtual reference.[36]

Unlike library registration and circulation records, virtual reference offers live digital transmission of data, and is susceptible to real-time intercept orders. These orders are given to the Internet Service Providers, and it is possible that the library will never even know the intercepts are taking place.

The privacy policy dilemna here is the same that is faced by libraries for any record, however. That is, *how* to let its users know. Should the privacy policy simply say, "These records will not be disclosed except as required by law" or should the message be highlighted more directly such as "Your records are subject to disclosure under the PATRIOT Act and related measures"?

D. Serious threats to life, limb or property and virtual reference privacy

Along the same vein, librarians are well aware that some of the 9-11 hijackers used public library terminals to buy tickets and plan their terrorist attack. After a librarian in Florida recognized pictures of the hijackers as branch library users, the library notified the FBI which got a proper judicial order before the library turned over the records.

But what if there simply is no time for legal process? Librarians have been confronted with users' messages like "I'm going to commit suicide" or "I'm going to blow up the library."[37] Should language from the Electronic Communications Privacy Act be used in the collaborative virtual reference policy explicitly allowing the librarian to disclose records when she believes in good faith that an ***emergency involving danger of death or serious physical injury*** requires disclosure without delay?

Would such language encourage librarians to overestimate the danger in requests for information on bomb-making and the like, which don't present true emergency situations?

E. International collaboratives

Privacy may be one of the more complicated issues facing international collaboratives. As mentioned in Section II, some nations restrict the transborder flow of personal data. Further study should be made of Europe, Canada and other nations to determine if contract language containing data protection language can satisfy international requirements.

F. Authentication without identification

> "[T]he new information age is turning out to be as much an age of information *about* readers as an age of information *for* readers."
>
> - Julie E. Cohen, law professor at Georgetown.[38]

Can or do any vendors provide authentication without identification? For example, is there a method that allows a user to type in identifying information such as a barcode and PIN, but breaks any further linkage to his searches? Is the Shibboleth project in use, or would it be helpful? From the Shibboleth site:

> **Active Management of Privacy**. The Identity Provider (origin) site, and the browser user, control what information is released to the Service Provider (target). A typical default is merely "member of community". Individuals can manage attribute release via a web-based user interface. Users are no longer at the mercy of the target's privacy policy.[39]

Activity	**How it is done today**	**Problems with current approach**	**What Shibboleth could do**
Accessing digital library resources from off-campus	Proxy servers, shared passwords or no service	Proxy servers hard to maintain No access from home IP address-based restrictions easily compromised Privacy can be compromised if identity is inappropriately passed to library	Permits access directly to content without campus proxy server Requires campus authentication, though identity is not passed to library Be used by libraries for new licensing approaches to content

From Internet2. The Shibboleth Project at http://shibboleth.internet2.edu/

For further research on authentication without identification, see the work of David Chaum, founder of DigiCash and the work of Herbert Burkert, Professor of Public Law, University of St. Gallen, Switzerland and author of "Privacy-Enhancing Technologies: Typology, Critique, Vision"; Technology and Privacy: The New Landscape edited by Philip Agre and Marc Rotenberg; The MIT Press (Cambridge, 1997).

V. DRAFT Model Collaborative Virtual Reference Privacy Policy

Thank you for using the **ASKUS** library reference service. Please read this privacy policy carefully and acknowledge your acceptance by clicking "I accept."

Quick version:

Virtual reference communications between users and library staff are kept confidential and will not be disclosed except: (1) as needed to answer your question (including referrals outside the library), (2) with consent of the user, or (3) as required by law. Personal identifiers used at the log-in screen, such as name, email etc. are stripped from transaction records after 90 days. Note that if personal information is given in the text of an online chat, email, or similar transaction, it may remain as part of a transcript or database record.

Although it may be helpful to the library if you enter your personal information at the log-in screen, it is not required to ask the library your reference question. An anonymous option is available. However, if the librarian refers you to a proprietary database, it may become necessary to enter an authorized user card number and PIN to gain access. Upon authentication, your user card number will not be linked to your searches.

ASKUS is committed to protecting and respecting your privacy and adheres to the American Library Association (ALA) Library Bill of Rights, and its 2002 Privacy Interpretation**.** This policy draws on the ALA Model Privacy Policy, the ALA Ad Hoc Committee on Virtual Reference Draft Guidelines 5/2003, and the 24/7 Privacy Statement.

Long version:

Preamble: Collection, Purpose, and Use of Personal Information

What information does ASKUS gather about you?

When you decide to ask a librarian a question at the **ASKUS** site, you may be asked to provide your name, e-mail address, ZIP code, and other information. While none of this data is required, and you may choose "anonymous" for your session, we are often better able to answer your questions if you volunteer complete and accurate information. For example, we can direct you to your local library's database collection.

When you give us your e-mail address, a transcript of your session with the librarian will automatically be sent to your e-mail address at the conclusion of the session. This transcript is also sent to the library, so that we can improve our services and so that we can get back to you if we find additional information about your question.

We will not use these email addresses for any other purpose. We also ask for your email when you fill out our satisfaction survey, to let us know if our service is useful to you. Although you don't have to complete the survey, or give us your email address at that time, doing so will help improve our service, and would give us the ability to contact you in case you have requested more information.

We also collect IP addresses to help us understand how our audience uses our site, so that we can make our site better and improve our users' overall experience when they visit **ASKUS.** We use "session cookies" that contain bits of information from the Web sites we visit. We will assign your browser a cookie in order

to maintain the session with the librarian. It is only temporary, and lasts only as long as your session with the librarian. It won't tell us who you are. Only you can do that.

IP Addresses and Cookies

ASKUS collects IP addresses for the purposes of system administration and sometimes for authentication (depending on your library's policies). If you choose the “anonymous” option, the IP address will be blocked from our view.

Session Cookies are used on **ASKUS** to maintain your connection to us. When you accept our session cookies, we cannot use them to find out who you are or any other personal information about you.

How does ASKUS use your personal information?

ASKUS collects personal information to provide you, the user, with the best and most personalized Web experience possible and to provide our affiliated libraries with an efficient means to improve services to their clientele. In short, by knowing a little about you, **ASKUS** can deliver more relevant content to you while at our Web site. **ASKUS** keeps personal information for 90 days, and then deletes everything except the domain your email (e.g. aol.com) which is used for statistical purposes. **ASKUS** will not use your personal information for other purposes without your permission.

Notice and Openness

ASKUS will provide notice to users of your rights to privacy and confidentiality via this privacy policy. We may update this policy from time to time so please check back periodically. We will prominently post any substantive changes in our privacy policy prior to implementing them. You can always review the most current version at http://www.askus.org/privacy.html

Will ASKUS disclose any of your personal information?

ASKUS will disclose your personal information only to the extent necessary to fulfill your request for information. For example, we may need to refer your question to a librarian in our network, who will have access to your information in order to get back to you with an answer to your question. We do not give, rent, lend, or sell individual information to any advertisers or other parties.

We may disclose aggregate information (for example, 5 million of our library users clicked on our site last month) in order to describe our services to our library partners and other third parties, and for other lawful purposes.

We employ contractors to help with our operations. Some or all of these contractors may access the databases of user information. These contractors are subject to confidentiality agreements that restrict their use and disclosure of all information they obtain through their relationship with **ASKUS**. Except as described in this Privacy Statement, or to comply with applicable laws or valid legal process, or to protect the rights or property of **ASKUS**, we will not disclose any personal identifiable information about our users.

The PATRTIOT Act and other provisions of law may require disclosure without notifying the user. Further, we may need to disclose your information if we have a reasonable belief that there is a serious immediate threat to life, limb or property.

Choice and Consent

May I be anonymous?

Yes, up to a point. We allow an anonymous option when signing in and asking questions. Often we can answer questions by pointing you to publicly available resources. However, sometimes our sessions lead to proprietary databases, and at that point, you will likely need a library card and PIN number to enter the database.

Are Children Treated Differently?

We would like children under 13 to ask their parents before giving out personally identifiable information. For that reason, we ask users to check a box stating that they are either 13 years old or over, or that a parent is present.

Why do you ask for permission to use my transaction?

It would be helpful to have sample transactions to use for promotion or other purposes. If you opt in to allow us to use your personal information, that could be helpful to us. If you do not, we will not use your PII, although we might use the text of the transcript for training, research, or other purposes. Any transcripts used for research and/or publication will conform to the Federal Policy for the Protection of Human Subjects (45 CFR 46) so that no personally identifiable information is ever made public.

Access by Users

Can I see my transaction?

Yes, we will automatically email you a copy of the transaction, if you give us an email address. If you choose the anonymous option, we will give you a URL that has the full text of the transaction.

We will give you additional information that we might have connected to you (e.g. your browser type, IP address) upon request.

How Can You Deactivate Your Account or Edit the Information We Have About You?

If you want us to delete any information in our databases that links you to your previously asked questions, you should contact **ASKUS**'s site coordinate privacy@askus.org. We do not otherwise keep user profiles.

Data Integrity and Security

What Kind of Security Measures Do We Take to Protect Your Information from Accidental Loss or Disclosure?

ASKUS is committed to protecting your personal information. All information that you provide to us is stored on our secure servers. If you are using a computer that others have access to such as one in a computer lab, Internet café or public library, always remember to log out and close your browser window when leaving our site. [Add statement about encryption here if it is used]

Enforcement & Redress

We enforce these privacy guidelines by contract with any third parties that share this information.
If you have any concerns or complaints, please contact **ASKUS**'s site coordinator at privacy@askus.org.

What Else Should You Know About Your Privacy?

While we do our best to protect your personal information, **ASKUS** cannot ensure or warrant the security of any information you transmit to us, and you do so at your own risk.
What does all this mean? Just as in the investing world, you must protect yourself. Please be careful and responsible whenever you're online.

Our librarians will routinely send you to other sites on the Internet. If you follow these links from our site to theirs, you should be aware that these other sites have their privacy and data collection practices. **ASKUS** has no responsibility or liability for these independent policies. For more information regarding a site and its privacy policies, check that site.

---

[1] See American Library Association Core Values Statement, *Protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship*, at < http://tinyurl.com/agrlq,>, citing *Libraries, an American Value*, adopted by the Council of the American Library Association, February 3, 1999 at <http://tinyurl.com/atjuc>. See also American Library Association, *Policy concerning Confidentiality of Personally Identifiable Information about Library Users*, adopted July 2, 1991; amended June 30, 2004, by the ALA Council at <http://tinyurl.com/38db8>.

[2] Paul Neuhaus, *Privacy and confidentiality in digital reference. Current issues*, REFERENCE AND USER SERVICES QUARTERLY, Fall 2003 at.26.

[3] Marc Rotenberg, *Privacy and transparency*, RLG NEWS, Fall 2001 at <http://www.rlg.org/en/pdfs/rlgnews/news53.pdf>.

[4] See *Senate Committee Approves Patriot Act Revisions*, AMERICAN LIBRARIES ONLINE, June 10, 2005 at <http://www.ala.org/ala/alonline/currentnews/newsarchive/2005abc/june2005a/patriot.htm>.

[5] For example, "tens of thousands" of user records were compromised at Georgia Southern University on April 28, 2005 by a hacker. Eighty thousand records were compromised May 7, 2005 when a laptop was stolen from the U.S. Department of Justice. See Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported since the ChoicePoint Incident*, at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

[6] American Library Association, *Privacy Tool Kit*, May 2, 2005 at <http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacytoolkit.doc>.

[7] For further insight, see Ann Bartow, *Libraries in a Digital and Aggressively Copyrighted World: Retaining Patron Access through Changing Technologies*, 62 OHIO STATE LAW JOURNAL 821 (2001) at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=555841>. Bartow argues that copyright law should be configured to guarantee library patrons the right and ability to use digital publications in the same ways they have used traditional formats: "Patrons should have the ability to read anonymously; to perform the electronic equivalent of pulling and rifling selected books, and also those adjacent on the shelf to a target publication; to place holds on desired publications already in use by others; and to freely check publications out for reasonable intervals of time, with the tacit understanding that they may choose to make fair use copies of excerpts, or even entire works, at their discretion, guided by the dictates of their consciences."[citation omitted].

[8] Gary T. Marx, *What's in a name? Some reflections on the sociology of anonymity*, THE INFORMATION SOCIETY, Special Issue on Anonymous Communication (1999), at <http://web.mit.edu/gtmarx/www/anon.html>.
[9] *Id.*.
[10] See, for example, Pam Davis, *The honor system: a library encourages kids to take books without checking them out*, SCHOOL LIBRARY JOURNAL, March 2004 at 41.
[11] Electronic Privacy Information Center (EPIC) and Privacy International, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS, (2004), at <**http://tinyurl.com/3upmm>.**
[12] *Id.* at <**http://tinyurl.com/74ddv>.** See for example, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, at <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>, Article 12 of the Council of Europe's 1981 Convention at <**http://tinyurl.com/ax7pq** > , Article 25 of the European Directive at <http://tinyurl.com/d93d>.
[13] See *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979) discussed in the context of reading records in Jared N. Klein, *Note: The Right to Privacy in what you Read: The Fourth Amendment Implications of a Book Store Search*, 13 TEMPLE POLITICAL & CIVIL RIGHTS LAW REVIEW 361, (Fall 2003).
[14] *Internet Privacy: Overview and Pending Legislation*. [RL31408] Marcia S. Smith. Library of Congress. Congressional Research Service. Updated March 16, 2005 at <http://www.ipmall.info/hosted_resources/crs/RL31408_050316.pdf>.
[15] 5 U.S.C. § 552a (2005).
[16] In June 2000, the Clinton White House revealed that contractors for the Office of National Drug Control Policy had been using persistent "cookies." A September 5, 2000 letter from the Office of Management and Budget to the Department of Commerce clarified the policy restricting persistent cookies. See *Internet Privacy: Overview and Pending Legislation*. [RL31408] Marcia S. Smith. Library of Congress. Congressional Research Service. Updated March 16, 2005 at <http://www.ipmall.info/hosted_resources/crs/RL31408_050316.pdf>.
[17] See for example, Federal Library and Information Center FLICC Newsletter (Spring/Summer 2004) at < http://www.loc.gov/flicc/pubs/fn0402.pdf> describing an all-day session on the E-Government Act, held at the Library of Congress, featuring Patrice McDermott, Deputy Director of the American Library Association Office of Government Relations. E-Government Act of 2002, (P.L. 107-347) 44 U.S.C. § 36 at < http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>.
[18] See Office of Management and Budget, Memorandum for Heads of Executive Departments and Agencies, M-03-22 from Joshua B. Bolgen, Director (September 26, 2003) at <http://www.whitehouse.gov/omb/memoranda/m03-22.html >.
[19] The standard machine readable format, Platform for Privacy Preferences, (P3P), has been developed by the World Wide Web Consortium seeks to provide an automated method for users to quickly compare a site's privacy policies with their own privacy preferences. P3P has been dubbed "Pretty Poor Privacy" by the Electronic Privacy Information Center which says that P3P fails to comply with baseline standards for privacy protection. Electronic Privacy Information Center, *Pretty poor privacy: An assessment of P3P and Internet Privacy*, (June 2000) at http://www.epic.org/reports/prettypoorprivacy.html. See further criticism that P3P does not minimize PII collection and in fact facilitates privacy concessions by users by Ruchika Agrawal, *Why is P3P not a PET?*, Electronic Privacy Information Center submission to W3C Workshop on the Future of P3P, (12-13 November 2002), Dulles, Virginia, USA at http://www.epic.org/reports/p3pnotpet.pdf. See also *Make your web site P3P complaint: How to create and publish your company's P3P policy (in 6 easy steps)*, W3C Platform for Privacy Preferences at http://www.w3.org/P3P/details.html.
[20] 18 U.S.C. § 2701 et seq. See especially §2711 for the definition of a "remote computing service," and §§2702-2703 for disclosure of customer records. For application to the library environment, see Mary Minow, *Could you be sued for turning over an Internet user's sign-up information to law enforcement? A cautionary tale for libraries and other Internet service providers*, LLRX.COM, April 26, 2004 at http://www.llrx.com/features/internetsignup.htm.
[21] 18 U.S.C. §2702(b)(7).

[22] 20 U.S.C. § 1232g; 34 CFR Part 99 available at < http://www.ed.gov/policy/gen/reg/ferpa/index.html>.
23 Complete lists of state confidentiality laws are available at American Library Association, *State Privacy Laws Regarding Library Records* at <http:www.ala.org/alaorg/oif/stateprivacylaws.html> and at *State Laws on the Confidentiality of Library Records*, compiled by Paul Neuhaus at <http://www.library.cmu.edu/People/neuhaus/state_laws.html> Note: Neuhaus guides readers to sources to find current versions of state law at state law websites.
[24] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6505. The FTC's final rule implementing the law became effective April 21, 2000 at <http://www.ftc.gov/os/1999/10/64fr59888.htm>. The law allows industry groups or others to develop self regulatory "safe harbor" guidelines that, if approved by the FTC, can be used by websites to comply with the law. The FTC approved self-regulatory guidelines proposed by the Better Business Bureau on January 26, 2001. Internet Privacy: Overview and Pending Legislation. [RL31408] Marcia S. Smith. Library of Congress. Congressional Research Service. Updated March 16, 2005 at <http://www.ipmall.info/hosted_resources/crs/RL31408_050316.pdf>.
[25] American Library Association, *Children's Online Privacy Protection Act* at http://www.ala.org/ala/washoff/WOissues/civilliberties/coppa/Default2434.htm .
[26] For further discussion on the anomalies of FERPA as applied to library records, see Helen Adams, Robert F. Bocher, Carol A. Gordon, and Elizabeth Kessler, PRIVACY IN THE 21ST CENTURY: ISSUES FOR PUBLIC, SCHOOL, AND ACADEMIC LIBRARIES (Libraries United 2005).
[27] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, (March 2002) at <http://www.epic.org/reports/dmfprivacy.html>.
[28] Marc Rotenberg, email to Mary Minow June 14, 2005.
[29] The FTC consent order, *In re Gateway Learning Corp*, FTC File No. 042-3047 (July 7, 2004) at http://www.ftc.gov/os/caselist/0423047/0423047.htm is discussed in Justine Young Gotshall, *Privacy Policies: Beware of Changes*, MODERN PRACTICE: FINDLAW'S LAW PRACTICE & TECHNOLOGY MAGAZINE, (March 2005) at <http://practice.findlaw.com/tooltalk-0305.html>.
[30] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete,"*(March 2002) at <http://www.epic.org/reports/dmfprivacy.html>.
[31] Checklist of Points to be Addressed in a CLD License Agreement at <http://www.cdlib.org/vendors/CDL_DB_Vendor_Req.rtf>.
[32] California Digital Library, *Technical Requirements for Database Vendors*, June 5, 2001, Latest revision October 28, 2004 at <http://www.cdlib.org/vendors/CDL_DB_Vendor_Req.rtf.>
[33] ABC-CLIO Privacy Policy at <http://www.abc-clio.com/privacy_popup.html.>.
[34] Paul Neuhaus, *Virtual Reference Software and Privacy Features*, (created December 2002. Updated August 19, 2004) at <http://www.library.cmu.edu/People/neuhaus/software.html>.
[35] *Tacoma Pub. Library v. Woessner*, 90 Wn. App. 205, 216-17 (1998).
[36] See for example, American Library Association, *Confidentiality and coping with law enforcement inquiries: Guidelines for the library and its staff, USA PATRIOT Act: What to Do If Served with a Search Warrant*, and other resources at <http://www.ala.org/ala/oif/ifissues/usapatriotactlibrary.htm>. See also Lee S. Strickland, Mary Minow and Tomas Lipinski, *Patriot in the Library: Management Approaches When Demands for Information are Received from Law Enforcement and Intelligence Agents***,** 30 NOTRE DAME JOURNAL OF COLLEGE AND UNIVERSITY LAW, 363 (2004) at <http://www.cip.umd.edu/publications/patriot_in_the_library.pdf > and Mary Minow, *Sample of search warrant procedures for libraries*, LLRX.COM (May 19, 2003) at <http://www.llrx.com/features/draftsearch.htm>.
[37] All of these typed messages have been seen by librarians, as reported to the author.
[38] Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996)
[39] Shibboeth Project at http://shibboleth.internet2.edu/.