

Privacy in Libraries, (ALTA, June 2004)

Carolyn Caywood

Thank you for this opportunity. I am especially honored to speak with library trustees and advocates because I have had recent experience of the importance of your role as the citizens' voice. Our local law enforcement asked the library to set up and retain logs of Internet use that they could check to see if anyone was accessing child pornography. Our attorney, who had previously supported us on other issues, counseled us to change our policy and comply. We turned to the Library Board, who saw the implications of a public record that, once created, could be used in unpredictable ways and who voted against creating these records. Their courage and wisdom affirms the important role of citizen boards. For me, the incident highlighted four important issues:

1. The necessity of a current policy -- ours is undergoing revision to catch up to new technology and the new ALA policy;
2. The importance of understanding public records retention & FOIA, as well as court orders;
3. The value of an informed Board and awareness & training for all who work with confidential information;
4. The need for public information about and discussion of privacy issues.

Understanding privacy & confidentiality, content & behavior

Privacy In a library, privacy is "the right to open inquiry without having the subject or one's interest examined or scrutinized by others." This is intellectual, not physical, privacy. It is secured through service planning as much as through policy. The best practice is to provide users with opportunities for informed choices and independent use. Choice is one of the *Fair Information Practices* that provide the structure for the model policy in the IFC's Guidelines for Developing a Library Privacy Policy. Attention to privacy can reduce our confidentiality responsibility by reducing the collection of personally identifiable information.

Confidentiality We are responsible for ensuring confidentiality when the library is in "possession of personally identifiable information about users and keeps that information private on their behalf." Personally identifiable information means both information identifying an individual and data that connects identification with interests. We have an active and ongoing responsibility to honor the public's trust. The best practice is to keep as little data as possible for as short a time as possible. What we must have, we must actively protect. This means not only technology and procedures, but

training for everyone who could compromise that protection.

Another important distinction is between behavior and content:

Behavior. Libraries have the right to make rules that protect safety, insure the care of the library's physical resources, and maintain an atmosphere conducive to study. Policies should show their tie to these reasons, which will help in publicizing them. Patrons have a right to know what the rules are and why they are necessary. They need to understand that libraries do not provide privacy for behavior. A library is a public place. It is inevitable that we will recognize some of our patrons. What we must avoid is letting what we know about their interests lead to assumptions about their behavior. And, of course, policies must be applied evenhandedly without prejudice. Library users should understand that breaking library rules can void their privacy protection, e.g. overdues or vandalism. If staff observe illegal behavior, they should report it to law enforcement. Nevertheless, libraries should avoid becoming involved in schemes to elicit and catch criminals.

Content. Courts have found a First Amendment right to receive information. The right to privacy and confidentiality is implied even though it is not stated. The Privacy Act of 1974 states that Federal agencies may not maintain records describing how any individual exercises rights guaranteed by the 1st Amendment unless expressly authorized by statute or by individual about himself or pertinent to law enforcement. A 1988 bill to protect library & video records was passed without the library provision because the FBI, was pushing elements of its "Library Awareness" campaign into the bill. Read Herbert Foerstel's *Refuge of a Scoundrel* (Libraries Unlimited, 2004) to follow developments from that campaign to today's USA PATRIOT Act. ALA's Privacy Interpretation asserts that a lack of privacy and confidentiality is a barrier to receiving information.

Recent developments that may affect Privacy Policies

Privacy an Interpretation of the Library Bill of Rights was adopted in June of 2002. Heretofore ALA policy dealt only with confidentiality. There are extensive resources on the ALA web site and the IFC continues to update the Privacy Tool Kit which includes the model policy and Guidelines for Developing a Library Privacy Policy mentioned earlier.

Information technology continually makes new opportunities for both privacy intrusion and protection, but more complexity means more uncertainty that the protection is effective. The Internet created an illusion of anonymity and heightened both expectations and fears of privacy. Technology has enabled commerce as well as government to mine data about individuals.

Information technology has also spawned non-technological threats like social engineering, shoulder surfing, and dumpster diving. Every library need a shredder! Bruce Schneier's *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Copernicus, 2003), offers excellent guidance for evaluating security, from home burglar alarms to Homeland Security. He makes it clear that we cannot rely on technology, we must heighten staff awareness of threats to the security of confidential data.

Information technology has made possible digitized databases and thus has created the opportunity for datamining. This is the retrieval and aggregation of personally identifiable information. At the same time, we are all well aware of the persistence of false information once it gets into a database, and the threats of hacking and identification theft. Despite evidence to the contrary, we tend to be far too uncritical of the accuracy of mechanized information. Nevertheless, the biggest threat is behavior prediction, that is, that the dataminers will think they can predict a person's actions based on a pattern in the data. In libraries, that means that they may equate reading interests with character. In addition, we ourselves face the temptation to misuse library data for library advocacy or fund raising. Not only is this a betrayal of public trust, it can backfire and create negative publicity. Any database used for library advocacy should be created through informed choice and kept separate from library use data.

In addition to digitized databases, other new technologies may be considered by libraries, like surveillance, biometrics, smart cards, and RFID. We must evaluate whether safeguards are adequate to protect confidentiality before adopting any new technology. I recommend the Harry Potter rule, "Never trust something that can think for itself if you can't see where it keeps its brain!" With all technology, plan for regular review to make sure it has not been compromised by continuing technological development. An especially important function of policies is to prevent "function creep" - collecting or sharing data for other agencies' purposes. Each new technology is liable to raise this temptation.

Finally, the societal pendulum that was already swinging toward risk avoidance before 9/11 has increased in its wake. There is a higher tolerance for privacy intrusion, especially among those who expect that it will only impact others' liberty. Thus we must raise awareness that privacy invasion affects the innocent. Accurate risk assessment is among the least taught skills of critical thinking, thus terrorists and psychopaths loom larger in public awareness than risks to civil liberties or commercial snooping. Bruce Schneier's book shows how such misperceptions actually compromise our security.

Safety & security

We have a responsibility to insure safety in libraries. Begin with a behavior policy that supplements laws with time, place, or manner (but not content or viewpoint) rules.

When creating rules, consider the impact of unattended children issues. Publicize the rules and train staff on policy enforcement. Talk with local law enforcement, library counsel, and the library's governing body about expectations. Seek their advice on safety but weigh that advice against the library mission. Examine the facility for safety improvements. Focus on preventing crime rather than catching criminals.

The first step toward data security is Records Management - are your records retention statements congruent with the library's use of the data? Know your state's Freedom of Information Act - states vary. What resources does your state provide? The Virginia FOI Advisory Council offers training and advisory opinions. Library records and library communication may be public documents, unless specifically exempted. At the Federal level, the *USDoJ v. Reporters Committee for Freedom of the Press*, 1989 case states that since the purpose of FOIA is open government, access to personal records of private citizens does not serve that purpose. But, the Virginia FOI Advisory Council says the state law provides no protection except its 81 exemptions, one of which is library circulation records. Find out if it is possible in your state to FOIA a research question, a database search, or other non-circulation record. Investigate what protections may be possible, for example, we are offering informed choice to borrowers for email notification.

Remember always that library personnel are agents of government, and thus the First and Fourth Amendments apply to staff, volunteers, & governance! Spell out the privacy and confidentiality rights and responsibilities of staff, volunteers and trustees as government agents, as employees, and as library users. Include anyone who handles personally identifiable information in your library. People who are informed are less likely to embarrass the institution or resent its rules. Schneier has called people the "weakest link" in security, but shows that, when properly trained, they can be its strongest defense.

Data security also needs regular privacy audits. A privacy audit compares an organization's goals and promises of privacy and confidentiality with its practices. Regular audits protect confidential information from abuse and the organization from liability and public relations problems. Auditing examines how information about customers and employees is collected, stored, shared, used and destroyed. Involve all stakeholders and aspects of privacy, from information technology to public relations and don't forget vendors. Make changes official in the library's Records Retention Schedule.

Talk to local law enforcement before you must confront them over a request for confidential information. Understand their mission is different from the library's. Remember too that libraries enjoy the greater public confidence! Explain library ethics - we facilitate, not monitor, access. Do not attempt to do their job of investigation and be clear that the library is not to be used. Explain why we require a court order for

disclosure - judicial review is an important Constitutional protection of individual rights. Preserving an uncompromised "chain of evidence" may be a common ground in the discussion. Also, talk with counsel as you develop policies. Train all staff, including pages, custodians, and volunteers to refer any request for confidential information to the appropriate authority. The library can move to quash a subpoena if it doesn't meet the Constitutional standard, "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

Minors' privacy rights may have extra legal protection from the Family Educational Right to Privacy Act (FERPA, or Buckley Amendment), and the Children's Online Privacy Protection Act of 1998 (COPPA). The Pico case stated that the right to receive information applies to minors. Often the issue of parental responsibilities is raised as a challenge to confidentiality. Make sure that staff take opportunities to communicate with families to clarify expectations. When the child's age makes it reasonable, urge parents to communicate with their children rather than to snoop on them. Think about the library's mission and potential unintended consequences, for example, my library issues cards for preschoolers too young to select books, much less to take responsibility for their return. Accept that families have changed and policies must accommodate joint custody and latchkey children.

Educating the public is key

Users have the right to be informed about library policy and to make informed choices. Confrontation is often the result of surprise and mistaken expectations. Policy should be stated on data collection forms with an explanation of why the data is needed and how long it is kept. Seek every opportunity to provide choices. Consider creating handouts on privacy in the library.

Users have a responsibility to respect each other's privacy. They should never be co-opted as content police. Library practices that turn users into informers invite trouble. Staff should model respect for privacy and interior design should reflect a concern for both privacy and safety.

Especially following the USA PATRIOT Act, the public has a critical need to understand privacy issues and risks and to learn how to protect personally identifiable information. Libraries can add materials and create web sites and bibliographies to help. Consider holding public forums on privacy issues. Privacy has good public relations potential and cuts across the usual ideological lines. It can be a foundation for broadening library support and public understanding.

Remember, above all, the necessity of policies to communicate the intent of the library, careful implementation of privacy protection and new technology, the importance of public records retention & FOIA, the necessity of training for all who handle confidential information, and the value of proactively creating opportunities for public information and discussion of privacy issues. Thank you.

Handouts

LIBRARY PROCEDURES THAT AFFECT PRIVACY AND CONFIDENTIALITY

Privacy

Directional signage
Open stacks browsing
Check out queue
Open access to library
Recessed/screened computer monitors
Ready reference, telephone reference
Open events
Self check out
Physical layout of stacks, seating

Confidentiality

Notice of policy on forms
Call slip requests
Circulation records
Patron records
Computer sign-up logs
Written up reference questions
Program registrations
Use of shredder
Reserve & overdue notification
i.e. mail, phone, or email

CHECKLIST of 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?

Planning for 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?

Privacy & Confidentiality Scenarios - what will you do?

1. The police have found library videos at a crime scene and subpoena their circulation records.
2. A phone caller asks you to page his wife who said she was going to the library.
3. You discover someone has inserted Polaroid photos of male genitalia in picture-books on the library shelves.
4. A patron reports that a man in a turban is looking at chemical formulas on the Internet.
5. A patron requests the floor plan of your library.
6. A woman phones to ask what is on her son's card so she can be sure she returns all his books.
7. An FBI officer presents a search warrant issued by the Foreign Intelligence Surveillance (FISA) Court.
8. A man calls and asks for the IP addresses of your Internet computers to aid in his search for a runaway who sent email home.
9. A state police officer presents you with a wanted poster and asks that staff call if they see the man who is presumed to be armed and dangerous.
10. A woman phones to ask if her ex-husband has registered their daughter for story time.
11. The arrest of a long-time library frequenter is extensively covered by the local news.
12. A patron asks for information on various methods of suicide.

Carolyn Caywood, MSLS
Bayside Area Library and Special Services

936 Independence Blvd. Virginia Beach, VA 23455
757-460-7519 ccaywood@vbgov.com

Privacy Resources and Commentary

Bielefield, Arlene. *Maintaining the Privacy of Library Records: a Handbook and Guide*. Neal-Schuman, c1994. Includes the background to support the professional position.

Branscomb, Anne W. *Who Owns Information?: from Privacy to Public Access*. Basic Books, c1994. Authoritative and scholarly.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Perseus Books, c1998. Looks at the imbalance of power over secrecy.

Cavoukian, Ann. *Who Knows: Safeguarding Your Privacy in a Networked World*. McGraw-Hill, c1997. Reviews the kinds of personal data likely to be part of large databases.

Computers and Society / Paul A. Winters, editor. Greenhaven Press, c1997. Covers privacy in a manner similar to *Opposing Viewpoints*.

Dolan, Edward F. *Your Privacy: Protecting it in a Nosy World*. Cobblehill Books, c1995. For young readers or as an overview.

Foerstel, Herbert. *Refuge of a Scoundrel*. Libraries Unlimited, 2004. FBI pursuit of library records from the '80s to the USA PATRIOT Act, with samples of Patriot warrants.

Garfinkel, Simson. *Database Nation: the Death of Privacy in the 21st Century*. O'Reilly, 2000. A grim analysis of mounting privacy risks with some prescient observations on terrorism.

Godwin, Mike, *Cyber Rights: Defending Free Speech in the Digital Age*. Times Books, c1998. Privacy is included.

The Information Revolution: Opposing Viewpoints / Paul A. Winters, editor. Greenhaven Press, c1998. A pro and a con essay on whether privacy is threatened by information technology.

Jennings, Charles, *the Hundredth Window: Protecting Your Privacy and Security in the Age of the Internet*. Free Press, 2000. Tips for reducing your exposure online.

Kennedy, Caroline, *The Right to Privacy*. Knopf, 1995. An analysis of its legal basis.

Lane, Carole A. *Naked in Cyberspace*. How to investigate other people: it includes a discussion of privacy and points out that you have to know how to find it to know how to hide it.

Lessig, Lawrence. *Code: and Other Laws of Cyberspace*. Basic Books, c1999. The architecture of the Internet determines the rights it fosters, according to Lessig.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in a Digital Age*. Viking, 2001. The evolution of encryption to PGP (Pretty Good Privacy.)

MccGwire, Scarlett. *Surveillance: the Impact on Our Lives*. Raintree Steck-Vaughn, 2001. An overview of the latest issues and technologies for young readers.

Minow, Mary and Tomas Lipinski, *The Library's Legal Answer Book*. ALA, 2003. Covers many issues including library records and privacy.

Mintz, Anne, ed. *Web of Deception*. Information Today, 2002. What to watch out for in Internet charity solicitations, legal advice, medical advice, fraud, misinformation, and privacy threats. The emphasis is on critical thinking skills.

Rosen, Jeffrey, 1964- *The Unwanted Gaze: the Destruction of Privacy in America*. Random House, c2000. Good historical background. Rosen theorizes that privacy has been sacrificed to punish discrimination.

Schneier, Bruce *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Copernicus, 2003. The computer security expert's test for everything from home burglar alarms to homeland security.

Tocci, Salvatore, *High-tech IDs: From Finger Scans to Voice Patterns* Franklin Watts, 2000. A simple overview of biometrics.

Privacy Viewpoints on the Web

Anti-Terrorism Legislation, Homeland Security, and Related Issues

<http://www.arl.org/info/frn/other/ATL.html>

Biometrics and Counter-Terrorism <http://www.ibia.org/Press%20Release%209.21.01.htm>

Developing a Confidentiality Policy <http://www.ala.org/alaorg/oif/frommanual.html>

Database Flaws Could Hamper National ID System, Experts Warn

<http://www.newhouse.com/archive/story1a122001.html>

FBI in Your Library <http://www.ala.org/alaorg/oif/fbiinyourlibrary.html>

Libraries and the Patriot Legislation <http://www.ala.org/washoff/patriot.html>

Library Records Post-Patriot Act <http://www.llrx.com/features/libraryrecords.htm>

Privacy and Confidentiality <http://www.ala.org/alaorg/oif/privacy.html>

Privacy and Consumer Profiling <http://www.epic.org/privacy/profiling/>

Privacy and Library Systems Before & After 9/11 <http://www.kcoyle.net/stbarb.html>

Privacy And Library Records Update: USA Patriot Act

<http://www.librarylaw.com/Patriotbib.htm>

Privacy Audit Checklist <http://cyber.law.harvard.edu/clinical/privacyaudit.html>

Privacy Commissioner releases finding on video surveillance (Canadian)

http://www.privcom.gc.ca/media/nr-c/02_05_b_011004_e.asp

Privacy Guidelines for Electronic Resources Vendors July 2002

<http://www.library.yale.edu/consortia/2002privacyguidelines.html>

Privacy Resources for Librarians, Library Users, and Families

<http://www.ala.org/alaorg/oif/privacyresources.html>

Public Libraries' Responses to September 11, 2001

<http://alexia.lis.uiuc.edu/~leighe/02PLA.ppt>

Questions and Answers on Privacy and Confidentiality

<http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/questionsanswers.htm>

Report of the CUL Task Force on Law Enforcement Access to Library Records

<http://www.library.cornell.edu/staffweb/LawEnforcementAccess.pdf>

Search & Seizure of Electronic Information: the Law Before and After the USA PATRIOT Act

<http://www.arl.org/info/frn/other/matrix.pdf>

State Privacy Laws Regarding Library Records <http://www.ala.org/oif/stateprivacylaws>

“Super Bowl Surveillance: Facing Up to Biometrics” by John D. Woodward Jr

<http://www.rand.org/publications/IP/IP209/IP209.pdf>

VA Freedom of Information Advisory Council <http://dls.state.va.us/foiacouncil.htm>

“Your Face Is Not a Bar Code” <http://dlis.gseis.ucla.edu/people/pagre/bar-code.html>

Revised 6/04