

Protecting Library Patron Confidentiality--Checklist of Best Practices

Trina J. Magi, Library Associate Professor, University of Vermont, Fall 2006

Note: This content is reprinted with publisher's permission from the following book: Magi, T. (2005). *Protecting our precious liberties: What every educator needs to know about libraries, privacy and freedom of inquiry*. Bloomington, IN: Phi Delta Kappa International.

Now that libraries have greater-than-ever potential for collecting and storing many types of personal data, often in digital form, librarians must be increasingly vigilant in guarding the public trust (Sturges et al., 2003). Fortunately, the library literature offers many concrete actions librarians can take to protect the confidentiality of library patrons, as listed below.

❑ **Conduct a privacy/confidentiality audit.**

Librarians should first review their everyday operations to make themselves aware of the many types of records that link patron identifiers with information requests. Examples include:

Circulation records

Overdue materials records

Interlibrary loan requests

Database search records

Requests for photocopy duplication

Request slips for materials in closed stacks

User profiles for selective dissemination of information (SDI) services

Records of Web pages visited on public terminals

E-mail messages sent and received on public terminals

Records of individual consultations with patrons

Copies of messages generated through e-mail or chat reference services

Sign-up sheets for use of computer terminals or other library resources

❑ **Gather the minimum amount of patron information needed for library operations (Drobnicki, 1992; Fifarek, 2002; Nolan, 1993).**

If the library needs to collect data about patrons for planning purposes, librarians should find a way to do so that protects the anonymity of patrons. For example, information could be collected in a separate database with no field for patron name or other personally identifiable information (Nolan, 1993).

❑ **Retain information connecting a user to a particular transaction only as long as needed for normal operations, and then discard (Nolan, 1993).**

As long as records of any type exist, librarians cannot ensure confidentiality, because the records can be obtained by government agencies. Experience shows that agencies *will* seek this information, and can do so more easily under provisions of the USA PATRIOT Act (Crawford, 2003). Crawford disputes many of the arguments made in favor of retaining records, and warns that we should be careful about giving up too much liberty in exchange for security. He suggests that librarians can continue to provide personalized services such as selective dissemination of information, but should ask for patrons' permission and tell them about the risks.

- ❑ **Restrict access to patron information to a limited number of appropriate library personnel, and don't give access or information to faculty or administrators (Nolan, 1993).**
- ❑ **Write use and privacy policies that tell patrons what they can do to protect their privacy, and acknowledge the limits of what you can do to protect them (Fifarek, 2002).**
- ❑ **Educate staff on confidentiality polices (Nolan, 1993). Also educate administrators, library board members, town officers and others whose support you will need.**
- ❑ **Make available a flyer or poster that states patrons' rights to privacy, possibly including the text of the applicable state law (Hidebrand, 1991).**
- ❑ **Rather than using sign-up sheets or otherwise creating records of people who use library computers, use a "pass system" in which the patron shows an ID to librarian, but the ID is not recorded (Minow & Lipinski, 2003).**
- ❑ **Avoid practices and procedures that place patron information on public view (American Library Association, 2004b).**
ALA advises librarians to (a) avoid using postcards to notify patrons of overdue or requested materials, (b) avoid giving the titles of reserve requests or interlibrary loan materials over the telephone to members of a library user's household or leaving such information on answering machines, and (c) be sure to position staff terminals carefully so that screens cannot be read by members of the public (American Library Association, 2004b).
- ❑ **If the library uses an outside Internet Service Provider, choose one whose practices best match the library's privacy policy (Minow & Lipinski, 2003).**
Minow and Lipinski (2003) observe that patrons' Internet activities and messages can be easily tracked and the library cannot control that information. Internet Service Providers, unlike libraries, may not have any incentive to resist government requests for patron information.
- ❑ **When using commercial document suppliers, make sure the library is not required by the agreement to identify the patrons who request information (Nolan, 1993).**
- ❑ **If the library buys an Internet filtering product, be sure company will not sell its database of Web sites visited by patrons in the library (Minow & Lipinski, 2003).**
- ❑ **Encourage the library consortia to which you belong to adopt privacy policies. Otherwise, you cannot guarantee the privacy rights of your patrons (Minow & Lipinski, 2003).**
- ❑ **Don't include patron names on interlibrary loan requests sent to other institutions (Nolan, 1993).**
Nolan points out that when requests are submitted to lending libraries, user information is often unwittingly shared with people outside the borrowing institution. He also raises questions about whether state laws concerning privacy include interlibrary loan records, and if so, which state law applies—the law in the borrowing or the lending institution's state? He advises that if the lending institution does not require the patron name, the requesting library should not provide it (1993).
- ❑ **Find ways to separate patrons' names from interlibrary loan records.**
Nolan asserts that the level of concern over confidentiality of circulation records has not been shown with regard to interlibrary loan records. "Interlibrary loan operations create a veritable blizzard of paperwork for most libraries. . . . Due to uncertainties of shipping, most libraries keep these different

pieces of interlibrary loan data for a considerable amount of time to help track and resolve potential problems" (1993, p. 81). Furthermore, interlibrary loan staff must keep for at least three years certain records about items they request in order to demonstrate compliance with copyright law (Coalition for Networked Information, 2002). There is no indication, however, that libraries must keep the *names* of the patrons who requested the interlibrary loan materials. Librarians should find ways to purge these names from the records they keep for the three-year period.

❑ **Set automated circulation systems to purge borrower information when items are returned (Drobnicki, 1992).**

Crawford warns librarians that the default in some automated systems is to retain circulation history, even after an item is returned. Librarians can change this, but they must first be aware that they need to do so. Crawford asserts that there is no excuse for maintaining circulation histories after items are returned and further believes there is no excuse "for a general-purpose library system that ships with retention of circulation history as a default, or even as an option without loads of warnings" (2003, p. 91).

❑ **Delete old Web server logs (Fifarek, 2002).**

Web log files store information about all the times Web pages are accessed, and may include such information as dates and times, URLs accessed, IP addresses or names of persons accessing pages, and whether or not the server successfully delivered the pages requested ("Web log file," 2001).

❑ **Check with software vendors to see if they have tools for making the library system logs anonymous (Fifarek, 2002).**

Many online library systems have the ability to log and track various uses of the system. For example, it may be possible to log every search performed in the online public access catalog.

❑ **On public workstations, use boot routines to clear caches, temp directories, and recent history browsing files (Fifarek, 2002; Minow & Lipinski, 2003).**

❑ **Use image programs to wipe out and recreate hard drives of public terminals each night. This will get rid of installed programs, cookies, and other identifiers, plus keep the machines in good working order (Fifarek, 2002).**

❑ **Delete cookie files or set browsers to reject cookies (Minow & Lipinski, 2003).**

References

- American Library Association. (2004b, March 5). *Privacy tool kit: Introduction*. Retrieved December 22, 2004, from <http://www.ala.org/ala/oif/ifttoolkits/toolkitsprivacy/Default4517.htm>
- Coalition for Networked Information. (2002, July 3). *CONTU guidelines on photocopying under interlibrary loan arrangements*. Retrieved September 30, 2004, from <http://www.cni.org/docs/infopols/CONTU.html>
- Crawford, W. (2003). Time for a privacy audit. *American Libraries*, 34(7), 91.
- Drobnicki, J. A. (1992). The confidentiality of library users' records [ERIC Document No. 358846].
- Fifarek, A. (2002). Technology and privacy in the academic library. *Online Information Review*, 26(6), 366-374.
- Hidebrand, J. (1991, January). Is privacy reserved for adults? Children's rights at the public library. *School Library Journal*, 21-25.
- Minow, M., & Lipinski, T. A. (2003). Library records and privacy. In *The library's legal answer book* (pp. 163-221). Chicago: American Library Association.

- Nolan, C. W. (1993). The confidentiality of interlibrary loan records. *Journal of Academic Librarianship*, 19, 81-86.
- Sturges, P., Davies, E., Dearnley, J., Iliffe, U., Oppenheim, C., & Hardy, R. (2003). User privacy in the digital library environment: An investigation of policies and preparedness. *Library Management*, 24(1/2), 44-50.
- Web log file. (2001). In D. Ince (Ed.), *A dictionary of the Internet*. Cary, NC: Oxford University Press. Retrieved January 4, 2005, from Oxford Reference Online database.