

INDIANA LIBRARIES AFFECTED BY USA PATRIOT ACT

by Steve Cochran



The Intellectual Freedom Committee of the Indiana Library Federation developed a "Question of the Year" questionnaire in late 2003 to poll Indiana libraries about a) their knowledge of the USA PATRIOT Act, b) whether the USA PATRIOT Act has resulted in any changes in privacy and confidentiality policies and procedures, and c) whether or not national security related inquiries about patron reading & Web browsing habits have been made since passage of the USA PATRIOT Act. (USA PATRIOT Act¹ is capitalized thus because it is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.)

In January of this year, the questionnaire was sent to all Indiana public libraries to ascertain what impact the passage of the USA PATRIOT Act has had on them, their patrons, and their policies and procedures. Of 238 public libraries, responses were received from 219, a 92% sample, which makes the information it provides highly representative.

The results should be cause for increased concern and caution by librarians in Indiana: Concern for the privacy and confidentiality of library customers, and caution in the development and implementation of policies and procedures to insure that patrons' access to the marketplace of ideas is not curtailed. The results further indicate a need for greater awareness of the requirements imposed on libraries and bookstores by the Act.

Question #1 was very carefully worded: "Since the passage of the USA PATRIOT Act in October of 2001, has your library received a visit from any law enforcement agency/agencies making national security-related inquiries about the reading/web browsing habits of any of your patrons?"² Check boxes provided for answering this question "yes," "no," or "not sure."

It was worded this way so that anyone answering would not be violating any restriction associated with any specific investigation. Section 215 of the USA PATRIOT Act prohibits libraries and librarians served with a Foreign Intelligence Security Act (FISA) warrant

from disclosing the existence of the warrant or the fact that records were produced as a result of the warrant. Answering this question does not require them to do either.

Nevertheless, it is apparent from answers received that the mere existence of the USA PATRIOT Act had a chilling effect on how straightforward the answers were. 1 library out of 219 – or just under one half of one percent – gave an unambiguous "Yes" to this question. Fortunately the responding librarian knew and had informed front-line staff about the gag order associated with Section 215 of the PATRIOT Act and had adjusted library policy as a result to include routinely erasing the history of patron checkouts, not archiving Internet sign-up sheets, and purging the history logs on Internet workstations.

2.75% of libraries surveyed (6 out of 219) answered "not sure," and fully 1/3 of these may have answered this way instead of answering "Yes," since they included comments to the effect that answering "yes" to the question would be in violation of the gag order.

Therefore, it is fair to surmise that at least .5%, and perhaps as many as 3.25% of Indiana libraries have "received a visit" from law enforcement authorities "making national security-related inquiries" into the information-seeking behaviors of library customers.

As would be expected, the vast majority (96%) of libraries have *not* been visited by law enforcement agencies in this regard.

Given the relatively high percentage of libraries experiencing inquiries, the answers to question 2 are cause for great concern. Sixty-four libraries – or 29% of the total – were unaware of the gag order associated with FISA warrants under Section 215 of the USA PATRIOT Act. Naturally, none of these had informed staff about the existence of the gag order, thereby putting their staff at risk of contempt, should a FISA warrant ever be served.

Answers to the 4th question were particularly surprising. This question asked "As a result of the USA PATRIOT Act, has your library made any adjustments in

its policies and procedures in order to minimize the amount of information available about your patrons' reading/Web browsing habits?"

Fully 64% (140) of respondents said they had made *no* adjustments to library policy as a result of the passage of the USA PATRIOT Act. Of these, only 7 (5%) commented that various privacy protection measures were in place prior to the passage of the Act.

The answers to questions about specific measures taken to protect patron confidentiality were also not encouraging:

- Nearly 29% of respondents indicated that they keep no history of patron checkout records once items are returned, but only one library gave a definitive "No" answer to this question. The rest left the question blank. This may come as a surprise to most public librarians, but many ILS systems *do* maintain a history log of patron checkouts, which only trained and knowledgeable IT staff can purge. Therefore, libraries shouldn't assume that a patron checkout history is not there just because it doesn't show up on the patron's record.
- 36% do not archive Internet sign-up sheets longer than necessary to compile statistical information.
- 8.2 % do not keep library card registration forms on file once patron data has been entered into the ILS.
- 25% delete the history logs on public access Internet workstations after each user logs off.
- Only 5% have adopted other privacy protection measures. Some that were mentioned include:
 - no longer retaining children's program registration logs.
 - logs of Internet Access on firewall are now purged every 10 days.
 - overdue notices now sent in envelopes instead of on postcards
 - ILL Forms are cleared out regularly now.
 - backup tapes are destroyed quarterly; current backup is kept in a safe.

The upshot here is that the privacy rights of most library patrons are *not* being adequately protected by Indiana's public libraries. Since they don't actively purge patron checkout histories, the vast majority of public libraries (falsely) make the passive assumption that if they cannot see the history of patron checkouts that history is not there. Most Indiana public libraries archive Internet sign-up sheets for much longer than necessary. Over 90% maintain records of paper library card application forms long after the need for them has

passed and three-fourths of Indiana's public libraries retain the history logs of their public access Internet workstations.

Libraries traditionally value protecting the privacy of their customers' reading and web browsing habits in order to encourage their customers to widely range throughout the spectrum of ideas available. Libraries also have long been guardians of the confidentiality of their customers' personal information; most librarians see it as a trust given them by their customers, which they violate at the risk of losing them. Yet the results of this survey suggest that a majority of Indiana's public libraries are not adequately safeguarding either the confidentiality of their patrons personally identifying information or the privacy of their reading and research habits. Why is this true?

An answer is suggested by one of the comments received: "if there is a suspected terrorist in our area, I wouldn't want to be the one protecting him/her." This respondent knew about the gag order, but *hadn't* informed front line staff about it, had made no adjustments to privacy policies, and didn't want any more information about the USA PATRIOT Act. Many librarians feel that while protecting privacy and confidentiality is a laudable thing, they don't want to be perceived as somehow standing in the way of the prosecution of the war on terror.

Thus, I see the need to offer a brief lesson in Constitutional democracy: a suspected terrorist is not a terrorist. Neither is a suspect in any particular crime a criminal. Our justice system presumes innocence until guilt is proven. Moreover, before anyone's private matters can be searched, an investigator has to show probable cause, or point to the existence of specific facts to support the belief that a crime has been committed or that the items sought are evidence of a crime.

In fact, it is, in part, the violation of this tenet of law by the USA PATRIOT Act that makes it so very objectionable: suspects are treated as if they are guilty. Not only that: we *all* are viewed as if we are potential terrorists. The standard of probable cause is discarded in favor of some vague belief that the materials sought *may* be related to an ongoing investigation related to terrorism.

The Attorney General has suggested that librarians are being "hysterical" in saying that the USA PATRIOT Act threatens traditional library values. Yet the Act is written so that many of the privacy rights of customers that we as librarians protect as a matter of course are indeed threatened. Moreover, the very idea that everything patrons check out or browse on the Internet can be scrutinized could have a chilling effect on their curiosity, if librarians do not act decisively to protect them through the development of appropriate policy and procedural safeguards.

The Intellectual Freedom Committee of the ALA published a paper in August of 2003 entitled *Guidelines for Developing a Library Privacy Policy* which lists several best practices for those libraries in the process of writing such a policy:

When developing and revising policies, librarians need to ensure that they:

- Limit the degree to which personally identifiable information is monitored, collected, disclosed, and distributed.
- Avoid creating unnecessary records.
- Avoid retaining records that are not needed for efficient operation of the library, including data-related logs, digital records, vendor-collected data, and system backups.
- Avoid library practices and procedures that place personally identifiable information on public view.³

The article includes a very useful checklist of questions for those who are developing such policies, which is included as Appendix B to this paper.

ABOUT THE AUTHOR

Steve Cochran (stevecochran@hotmail.com) is Chair of the Indiana Library Federation's Intellectual Freedom Committee and Director of the Alexandrian Public Library in Mt. Vernon, Indiana.

REFERENCES

¹ http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?Dbname=107_cong_bills&docid=f:h3162enr.txt.pdf (accessed September 12th, 2004)

² The first question was actually "What type of library do you represent?" but since all responding libraries were public libraries, this question is ignored. The questionnaire appears as Appendix A to this paper.

³ *Guidelines for Developing a Library Privacy Policy*, ALA Office for Intellectual Freedom, August 2003. <http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/guidelineslibraryprivacy.doc> (accessed October 1, 2004)

APPENDIX A

Question of the Year 2003: USA PATRIOT Act

The results of this questionnaire will be analyzed by the Indiana Library Federation Intellectual Freedom Committee, and the general results published as part of the committee's continuing efforts to increase public and professional awareness of the importance of free speech and free access to information. Your participation is voluntary; your cooperation is much appreciated.

Please answer the following questions in the spaces provided below. Make one copy of the completed questionnaire for your records; send the original with your completed annual report to:

Indiana State Library, 140 N. Senate Ave.,
Indianapolis, IN 46204-2296

1. What type of library do you represent? academic public special

2. Since passage of the USA PATRIOT Act in October of 2001, has your library received a visit from any law enforcement agency/agencies making national security-related inquiries about the reading/web browsing habits of any of your patrons?
 yes no not sure

3. Do you know that if you are served with a search warrant under the Foreign Intelligence Surveillance Act (FISA), it comes with an automatic gag order that prohibits your library from notifying the patron under suspicion, the press, or anyone else that an investigation is underway?
 yes no

4. If the answer to question 3 is "yes," have you taken steps to educate and inform your front line staff regarding this gag order, and the proper steps they should take if and when they are presented with such a warrant?
 yes no

5. As a result of the USA PATRIOT Act, has your library made any adjustments in its policies and procedures in order to minimize the amount of information available about your patrons' reading/web browsing habits?
 yes no

6. If the answer to question 5 is "yes," please indicate what steps you have taken.
 do not keep history of patron check-outs
 do not keep/archive Internet sign-up sheets
 do not maintain library card application forms once card is assigned
 computer history logs set to automatically purge after each logoff
 other – please explain _____

7. Would you like more information about the USA PATRIOT Act and how it affects your ability to protect your patrons' privacy and confidentiality?
 yes no

8. If you answered "yes" to question 7, please send your library's name and address to:

Patriot Act Info., Intellectual Freedom Committee, Indiana Library Federation,
941 E. 86th St., Suite 260, Indianapolis, IN 46240

APPENDIX B

Checklist of Basic Questions about Privacy and Confidentiality

Collecting Information

- Do we need to know this to operate the library?
- How long do we need to know it?
- How will we protect what we collect?
- How will we destroy what we collect?
- How will we inform the public about confidentiality?
- How will we give users choices?
- How will we inform/influence government acts that impact confidentiality?

Providing Privacy

- Where do users need privacy to protect their intellectual freedom?
- Where would privacy endanger safety?
- How will we provide privacy where we should?
- How will we ensure safety without being intrusive?
- How will we educate staff about privacy?
- How will we inform the public about privacy in libraries?
- How will we inform the public about library resources on privacy issues?
- How will we give users choices?

Reviewing Your Policy

- Does your policy statement explain the difference between privacy and confidentiality in a library setting?
- Does your statement make clear the role of confidentiality in protecting intellectual freedom?
- Is the information to be protected listed: reference requests, information services, circulation & registration records, server and client computer logs?
- Have you included language to deal with unforeseen circumstances, like "including, but not limited to..."?
- Does your policy require that library users be notified whenever their PII is collected by the library and be told how to correct inaccurate information?
- Do you state who may or may not have access to patron information?
- Do you outline the specific conditions under which access may be granted? i.e., with a court order after good cause has been demonstrated?
- Do you list the procedure for adopting the policy?
- Are there provisions for notifying the public of the policy?
- Are exemptions, exceptions, or special conditions enumerated?
- Do you address needs unique to your library environment?
- If your library is part of a cooperative, automated library system, are there provisions for coordination with the other libraries in your system?
- Is the procedure outlined for responding to court orders of various types?
- Are the Library Bill of Rights, Statement on Professional Ethics, ALA Policy on the Confidentiality of Library Records, and state & local laws (where applicable) mentioned or acknowledged? Does your policy conform to these supporting documents?