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

Table of Contents

I. Need for Policy 1

II. Activities of the Task Force 2
- Task Force Charge and Members
- Process
  - Interim Procedure
  - Meetings with Cornell Officials
  - Conferences at Cornell University

III. Summary of Recommendations 5
- Guidelines for Responding to Requests from Law Enforcement Authorities for Library Records involving Patron Data
- Policies on Patron Data Retention
- Training

IV. Policies and Procedures for Responding to Law Enforcement Requests for Patron Information 7

V. Identifying and Evaluating Patron Data Retention Policies 9

VI. Appendices

A. Libraries and the Patriot Legislation – ALA web site
http://www.ala.org/washoff/patriot.html

B. ALA Guidelines for Librarians on the U.S.A. Patriot Act: What to do before, during and after a "knock at the door?"
http://www.ala.org/washoff/patstep.pdf

C. The Search and Seizure of Electronic Information Matrix
http://www.ala.org/washoff/matrix.pdf

D. Office of Cornell Information Technologies Procedure and Protocols under the "USA-PATRIOT ACT" Exceptions to the Electronic Communications Privacy Act
http://www.cit.cornell.edu/oit/policymemos/PatriotAct.html

Need for Policy

The USA PATRIOT Act was passed by Congress as a direct result of the tragic events of September 11, 2001. The full title of the act describes its purpose: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. While libraries are not specifically mentioned in the act, libraries are subject to the new law regarding business records that can be obtained by law enforcement agents. Any records that law enforcement reasonably believes could have a terrorist connection - from circulation records to chat reference transcripts - could be requested. CUL has certain legal obligations that come from the new anti-terrorism legislation as well as professional concerns for privacy and information in a free society. To be ready to deal with our obligations and concerns, LMT has asked the Task Force to recommend library policies and procedures for implementation at Cornell.

Library staff are all familiar with state laws on confidentiality of patron records. The new federal law adds to the laws that control access to patron records. Because of the complexities in the laws, the essence of the recommended procedures is to contact University Counsel for advice before disclosing any information to law enforcement agents.

This policy deals specifically with patron record requests from law enforcement. Other important issues for CUL include questions of patron access to government information, which is addressed by CUL Policy on Returning or Destroying Materials on Request, February 14, 2002. A broad look at these issues is available in an April 8, 2002, Congressional Research Service report to Congress on "Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education," at http://www.aau.edu/research/crsterror.pdf
The text of the USA PATRIOT Act, Public Law 107-56, is available on the web at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

Activities of the Task Force

Task Force Charge and Members

In January 2002, the CUL Library Management Team established a task force, at the suggestion of the Public Services Executive Committee, to establish guidelines for responding to requests for library records, under the new USA PATRIOT Act. This charge was approved in March 2002:

> The Task Force on Law Enforcement Access to Library Records is established by the CUL Library Management Team. Members are Pat Court (Chair), Law Library; Surinder Ghangas, Digital Libraries and Information Technology; and Jesse Koennecke, Mann Library.
>
> The Task Force is charged with establishing guidelines for responding to requests from law enforcement authorities for library records involving patron data, keeping in mind the American Library Association Code of Ethics which recognizes that we protect each library user's right to privacy and confidentiality. In addition, the Task Force will recommend policies on retention of all types of patron records that are needed for the operation of the library.

Process

<u>Interim Procedure</u>

Because requests for patron data could come at any time, perhaps before final guidelines were in place, the Task Force suggested to LMT that all library staff be notified as soon as possible that there is a new law in place and that their responsibility was to immediately notify their supervisor, who would contact appropriate administrators who would get legal advice, if law enforcement requested any library records.

This message was sent to library staff through the cu-lib listserv on March 15 from Ross Atkinson, Associate University Librarian for Collections:

> Subject: Responding to rqsts for lib records
>
> Cornell University Library Staff:
>
> Recently passed laws and directives may have an impact on how CUL responds to requests for Library records from law enforcement authorities. This might include requests for circulation records, web use records, reference question logs, e-mail, etc. There is a Task Force working now to establish guidelines on our procedures.

Because such requests might be received before the Task Force completes its work, this message is to let you know in the interim what to do if law enforcement authorities request Library records from you. Inform the authorities requesting the information that you are not authorized to provide it, and you should then contact your supervisor. Do not disclose any information and treat the request as confidential.

Supervisors should contact a member of the Task Force on Law Enforcement Access to Library Records, who will be able to offer assistance. They will contact the Library Administration and the University Counsel's Office. The Task Force members may be contacted at work or at home

Pat Court (Chair), Law Library
office 5-5853
home 257-0942
e-mail pgc1@cornell.edu

Surinder Ghangas, Digital Libraries and Information Technology
office 5-0636
home 257-3907
e-mail sg14@cornell.edu

Jesse Koennecke, Mann Library
office 5-5680
home 272-0727
e-mail jtk1@cornell.edu

Thank your cooperation on this important interim procedure.

---Ross

Meetings with Cornell Officials

Two key offices at Cornell were identified as having important information for the library policies that were being developed. One is University Counsel, specifically attorney Pat McClary, who regularly advises CUL. The other is the Office of Information Technologies, specifically Tracy Mitrano, who is Policy Advisor for OIT and the Co-Director of Cornell's Computer Policy and Law Program.

The Task Force members met with Tracy Mitrano on April 9. Dr. Mitrano is recognized as a leading expert and in-demand speaker on the issues we are dealing with, since her office promulgated the "Office of Cornell Information Technologies Procedure and Protocols under the USA-PATRIOT Act Exceptions to the Electronic Communications Privacy Act," which is a model policy for universities and libraries across the country.

See Procedure at Appendix D. The OIT procedure follows the university-recommended procedure: staff does not give information to law enforcement; rather, staff contact one of the specified OIT administrators, who contacts University Counsel for advice.

Pat McClary met with members of the Task Force on April 17. The group wanted University Counsel to know that CUL was developing a written policy. Ms. McClary confirmed that it was essential to consult with their office before turning over any records or otherwise attempting to comply with an order presented by law enforcement agents. She encouraged CUL to have its own internal reporting procedures, which are at the discretion of the library to develop.

Conferences at Cornell

To learn more from local experts and to share concerns and potential solutions with other institutions dealing with issues of library information and security, Task Force members attended two conferences held on campus. Jesse Koennecke attended "Legal Issues in Information Security," the annual spring conference of the College and University Information Security Professionals, on April 15-17. Pat Court and Surinder Ghangas attended "May You Live in Interesting Times: Current Issues in Information Access," the annual spring conference of the Eastern New York Chapter of the Association of College and Research Libraries, on May 5-6. The information learned at these conferences on the specifics of the law and the practical actions suggested have been incorporated into the recommendations of the Task Force.

Summary of Recommendations

Guidelines for Responding to Requests from Law Enforcement Authorities for Library Records involving Patron Data

No library staff member at any level is expected to know how to evaluate a request from law enforcement agents for patron data. The possible responses to a subpoena, a court order, a search warrant, or other requests must be considered by attorneys. University Counsel needs to be brought in as soon as possible to review the request and advise on appropriate response. Therefore, the policies and procedures recommended by the Task Force name specific administrative positions within CUL to be contacted as soon as possible about any requests. The person in that position who is contacted should immediately contact University Counsel and the University Librarian. The responsibility of each CUL staff member is to be aware of the possibility of such requests; staff should not disclose any information. Each unit should have specific procedures on who should contact the CUL administrators. Staff can contact the CUL administrators directly or may, in accordance with unit procedures, refer request to a supervisor within the unit library, who would contact the CUL administrators.

The Task Force recommends that CUL carefully follow the suggestions of the American Library Association in their Guidelines for Librarians on the U.S.A. Patriot Act (see Appendix B for details):

Before:

- Consult Your Local Legal Counsel
- Review Your Policies
- Train Your Staff

During:

- Follow Your Procedures
- Consult Your Local Legal Counsel
- Document Your Costs

After:

- Consult Your Local Legal Counsel
- Follow Up

Policies on Patron Data Retention

There are decisions regarding patron data retention that can be made at the broad CUL level; other decisions need to be made at the departmental or unit level. The law does not specify what patron data must be kept, so if information is not needed for library business, it need not be retained. Records that identify library patrons should be identified and reviewed to determine the need for the information. See details in section V. Identifying and Evaluating Patron Data Retention Policies.

Training

The Task Force recommends that all CUL staff be trained in the new policy and procedures related to law enforcement requests for patron data. This report can be disseminated to staff through the cu-lib listserv and made available on the CUL staffweb. Information sessions conducted in the many functional committees and working groups would serve to pass on the information and handle questions from various groups. LMT may wish to have information sessions at Academic Assembly and in the groups that work through the Public Services Executive Group, the Technical Services Executive Group, the Collection Development Executive Group, and the Digital Library and Information Technologies Division. Members of the Task Force will be happy to meet with LMT and other groups to discuss procedures for handling information requests and review of data retention policies.

Policies and Procedures
for Responding to Law Enforcement Requests for Patron Information

Cornell University Library

Should an individual or individuals representing themselves as law enforcement agents approach you and ask you to provide library records involving patron data or information about library users with or without any form of written authorization, do not disclose any information. Contact any member of the Library Management Team, who will make the necessary communication to University Counsel's Office and the University Librarian. Also, contact the supervisor in your unit.

Library Management Team Contact Information

Ross Atkinson	Associate University Librarian for Collections		
	Office: 5-5181	Private: 5-5475	Home: 844-9307
Karen Calhoun	Assistant University Librarian for Technical Services		
	Office: 5-5752	Private: 5-9915	Home: 607-844-3533
Lee Cartmill	Director of Finance and Administration		
	Office: 5-5181	Private: 5-5472	Home: 257-7807
Claire Germain	Director of Law Library		
	Office: 5-5856	Private: 5-5857	Home: 257-2765
Tom Hickerson	Associate University Librarian for Information Technologies & Special Collections		
	Office: 5-9965	Private: 5-9556	Home: 257-6484
Anne Kenney	Assistant University Librarian for Instruction, Research, & Information Services		
	Office: 5-5068	Private: 5-6875	Home: 272-9137
Janet McCue	Associate University Librarian for Life Sciences & Director of Mann Library		
	Office: 5-2285	Private: 5-2795	Home: 607-387-9205
Jean Poland	Associate University Librarian for Engineering, Mathematics, & Physical Sciences		
	Office: 5-4016	Private: 5-6038	Home: 607-266-8079
Carolyn Anne Reid	Acting Director of Weill Medical Library		
	Office: 212-746-6069		Home: 212-988-5063
Sarah Thomas	University Librarian		
	Office: 5-3689	Private: 5-5474	Home: 257-8296
Edward Weissman	Assistant to the University Librarian		
	Office: 5-3393	Private: 5-5754	Home: 273-4415

1. Antiterrorist legislation signed into law in October 2001 and popularly known as the USA PATRIOT Act creates new responsibilities for required disclosures of business records to law enforcement. Cornell University Library needs to follow the advice of University Counsel on how to respond to requests for disclosure of library records.

2. Cornell University Library subscribes to the American Library Association Code of Ethics (http://www.ala.org/alaorg/oif/codeofethics.pdf), which recognizes that we protect each library user's right to privacy and confidentiality.

3. The fact of an information request, the nature of the request, and the names of library patrons are to be treated in the strictest confidence and are not to be discussed or revealed, according to the requirements of the USA PATRIOT Act.

4. Library records, which may be the focus of law enforcement requests, include electronic, print, and other forms of patron information. CUL and its unit libraries need to retain specific information for the regular operation of library business. Archives of information that reveal identities of individuals should be kept only when clearly necessary.

5. An exception to this policy provided for by the USA PATRIOT Act allows voluntary disclosure for emergency situations, which are likely to be rare in the library. Should a staff member, in the course of business, reasonably believe he has accessed information about an emergency involving immediate danger of death or serious physical injury, he should contact the university police immediately ; then contact any member of the Library Management Team and the supervisor in the unit.

6. Each unit is responsible for adherence to this policy and procedure. All library staff, including student assistants, are to be fully informed on this policy and procedure and need to understand their own role if such situations arise.

7. Any questions about these procedures should be addressed to the Director of Finance and Administration at (607) 255-5181.

July 10, 2002
Updated July 25, 2002

Identifying and Evaluating Patron Data Retention Policies

Cornell University Library

Throughout day-to-day operation, CUL and its individual unit libraries gather a large amount of data regarding patron use of materials and information. A lot of these data remain anonymous in the form of statistics, but, by necessity, certain amounts retain a direct connection between an individual and their specific information use. These data may be part of current open transactions, needed for detailed analysis, or held within a back-up system and therefore it may be important to retain the patron to information connection.

It is important to identify and evaluate the patron-related data kept by CUL, both centrally and within the individual departments and units libraries. The library is under no legal obligation to log or retain patron associated information, but could be forced by warrant or subpoena to make available any or all of these data. Identifying and evaluating data retention policies will provide two benefits. It will:

1. Limit the total amount of available data to those that are necessary to conduct business and further development, and

2. For legitimate investigations, as determined by University Counsel, the library will know exactly what and how much data are available.

Example: Within the Voyager database, unless there is a fine associated with a transaction, the link from item to patron is lost the moment an item is discharged. It has been determined that a fine must be associated with both a patron and an item to remain enforceable. Without a fine, the patron to item connection is less important than the possible privacy concerns that could arise by keeping records of what patrons formerly charged-out.

Example: CUL keeps back-ups of the Voyager database for thirty-five days. These are important to minimize data loss in the event of a system failure. When the time has expired, the data are deleted and written over. It has been determined by the library systems department that this thirty-five day window is needed to best protect the Voyager database.

Identify: Both centralized departments and unit libraries should examine the information they keep where a patron could be directly associated with items or information. These data could include original and back-up versions of:

- Patron E-mails – Whether circulation notices, reference questions, or other e-mails to and from patrons, these can contain detailed data regarding patron information and materials interests and use.
- Chat logs – E-reference chat logs can link patrons with information requests.

- Local databases – Any gathering of patron-to-information data that are kept outside of the LMS or other central CUL managed database. These might be billing information outside of Voyager or Table of Contents services.
- Paper or manual files – Whenever patron transactions are documented in notebooks, McBee cards, log sheets, etc. Sometimes these are retained long after the transactions are complete.

Evaluate: Once identified, these data collections should be evaluated. The inherent value of the data should be weighed against the importance of patron privacy. Where it is deemed unnecessary to retain a direct relationship between patron and information use, policies and procedures should be developed to delete the data, or remove the patron connection.

Relevant questions to consider might include:

How long is this needed?
What is its purpose?
Can statistics be gathered, then the data deleted?
Can patron identity be removed without compromising the usefulness of the data?
Is this information or process duplicated elsewhere?
What technical concerns are there for retaining or deleting these data?
Is there any mandate to retain or delete these data?

July 10, 2002