Mary Riley Styles Public Library

LIBRARY POLICY MANUAL

ADM-11 Confidentiality Policy and Responding To Judicial Process

Date Issued: 10/18/89; Revised: 9/18/96; 6/18/03
Attachment(s): None

1. Definitions

Judicial process: A general term used to encompass a complex array of demands for information under the authority of a court or judicially-related process.

Search warrant: Issued and signed by judges or magistrates on behalf of government prosecutors in criminal matters and give the executing officers broad authority to secure the listed information. Issued after a determination of probable cause and is served and executed immediately by law enforcement officers with or without one's cooperation.

Subpoena: Can be issued in civil or criminal cases and on behalf of government prosecutors or private litigants; often, subpoenas are merely signed by a government employee, a court clerk or even a private attorney. A subpoena merely asserts that information is relevant to a judicial matter, requires one to produce records at a specific future time, and may be contested by the library through a Motion to Quash.

National security letter (NSL): A type of administrative subpoena that is issued independently by Federal Bureau of Investigation (FBI) field offices and is not subject to judicial review or a show of probable cause unless a case goes to court. It can be used to obtain records from financial institutions and Internet Service Providers (ISPs), web mail providers, and other communications service providers. The people whose communications are searched are not notified, and every letter is accompanied by a gag order that prohibits the letter's recipient from ever revealing its existence.

Intercept order: A judicial written order that allows the federal government to intercept or seize in transit electronic information. It must be signed by a federal judge, must be pre-authorized by the U. S. Department of Justice and is limited to 30 days and renewable for 30 more days. If it is a request under the Foreign Intelligence Surveillance Act (FISA), a gag order accompanies it.

Electronic Communications Privacy Act (ECPA): An act that permits an "electronic communications service" (ECS) provider to the public and a "remote computer service" (RCS) provider (in this case, the library) to the public

to monitor their system for management purposes and to disclose content and other information in the following very limited circumstances: 1. as necessary to protect the property of the library/City; 2. if related to the commission of a crime, or 3. if related to an emergency involving immediate danger of death or serious physical injury. It also authorizes a government or private employer to monitor use of electronic systems by its employees. The USA Patriot Act broadens ECPA's definition of "tangible items" to include real-time interception of non-content electronic information (dialing, routing, etc.) and real-time interception of the content of electronic communications.

Foreign Intelligence Surveillance Act (FISA): An act that authorizes FBI agents conducting foreign intelligence investigations to wiretap, conduct physical searches or use instruments to secretly identify the source and addresses of telephone calls made to and from a particular telephone. The USA Patriot Act broadens FISA's definitions of "tangible items" to include e-mail (opened and unopened), stored voice mail transmitted by computer, transaction and account records, and basic subscriber information (name, address, etc.).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 aka USA PATRIOT Act: A federal law (HR-3162, Public Law 107-56) that was enacted on October 26, 2001, in response to the terrorist attacks on September 11, 2001. Federal authorities engaged in gathering foreign intelligence information or conducting an investigation of international terrorism, can seek a court order to access hotel, airline, storage locker or car rental records. The businesses to whom the orders are addressed are bound to silence. The act broadened access to "any tangible item no matter who holds it." It contains no provisions specifically directed at libraries or their patrons. However, **it has several provisions that allow the federal government to have access to records from any source, including libraries.**

2. Policy

It is the policy of the Mary Riley Styles Public Library that circulation records and other records identifying the names of library users with specific materials are confidential. Such records shall not be made available to any agency of state, federal, or local government or any individual except pursuant to such process, order, or subpoena as may be authorized under the authority of, and pursuant to, federal, state, or local law relating to civil, criminal, or administrative discovery procedures or legislative investigative power. Upon receipt of any process, order, or subpoena seeking library records, the Library Director and the City Attorney of Falls Church shall determine if such process, order, or subpoena is in proper legal form.

Library personnel shall not disclose the library's circulation records and their

contents (whether in paper or electronic format) as pertaining to individual patrons, the library's patron records and their contents, the number or character of questions asked by a patron, the frequency of a patron's visits to the library, or a patron's name, address, or telephone number to any other individual, corporation, institution, government agent, or agency except as provided in the first paragraph or under the options that apply to parents of children under the age of 14. Furthermore, library personnel shall not disclose any other library service records that reveal the details, nature, or purpose of information requested or obtained by an identifiable patron unless required by the Virginia Freedom of Information Act, subpoena, court order, or similar order, or unless disclosure of the information is specifically approved by the Library Director or her designee.

If a search warrant is issued pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 *U.S. Code* 1861, the Library Director shall take measures to ensure that only those library staff who are necessary to produce the records or assist in the search are informed of the warrant or national security letter. The Library Director shall advise those library staff members that federal law prohibits them from disclosing the existence of the search warrant or national security letter.

With the advent of the USA Patriot Act, the library notifies patrons that "Under Section 215 of the federal USA Patriot Act (Public Law 107-56), records of the books and other materials they borrow from this library may be obtained by federal agents. That federal law prohibits librarians from informing a patron if records about him/her have been obtained by federal agents."

While the library does not monitor on a routine basis the use by patrons or staff of its electronic systems, the library does follow the Electronic Communications Privacy Act. The library reserves the right to: 1. monitor, as necessary, to manage and protect its systems from unauthorized or criminal use; and, 2. disclose to federal and state law enforcement and national security authorities as deemed appropriate by library management and the City Attorney. Therefore, at each workstation the following sign is posted for both the public and employee's information: "Activity on this computer may be monitored according to state and federal law." This statement also appears at the time a workstation reservation is placed on the Pharos server by a patron.

Patrons of all ages have the right to receive information about their own records, but must first provide personal identification. Acceptable identification includes their library card, driver's license, or validation of personal information in the patron's record.

The following options apply to parents of children under the age of 14. At the time of registration or thereafter by re-registration, the parents must indicate in writing what option they and their child jointly choose.

- Parents of children under the age of 14 may opt for full confidentiality of their child's circulation record. Full confidentiality means that no one other than the child has access to the record.

- Limited access cards allow parents of children under the age of 14 to ask for and receive information about lost, damaged, or overdue items if the child is present or has given prior written consent. If both parents want access to the record, both parents must sign the child's registration form (sample attached) stating such. Parents must present acceptable identification that matches the name(s) on the child's patron record in order to see the child's record.

- Full access cards allow parents of children under the age of 14 to have access to all of their child's circulation records upon presentation of acceptable identification that matches the name(s) on the child's patron record. If both parents want access to the record, both parents must sign the child's registration form stating such.

Please note that all circulation records only contain what materials are currently checked out and what fines and fees are attached to the record. No historical information is kept regarding what someone has read.

Patrons who wish to pay fines for other family members may be told only the amount due if the fines belong to a patron age 14 and older.

Information provided over the telephone shall be limited to the number of items charged to a patron and the amount of the fines for all patrons, after the solicitor has given his name and library card number.

Any problems or conditions relating to the privacy of a citizen or patron through the records of the Mary Riley Styles Public Library which are not provided for in this policy statement shall be referred to the Library Director, who upon proper study of the issues and in consultation with the City Attorney and the Board of Trustees, shall determine the response to the request.

See also Resolution 2003-16 and sample copies of court orders for Washington DC and Virginia (attached). See also the Library's Website and Privacy Policy.

IV. Procedures for Protecting Library Information and Responding to Judicial Process

The following procedures set forth the steps that each member of the Library staff must follow in responding to a judicial process situation. The Library Director is the only authorized person to accept these requests, however, in her absence, the person in charge may, but must inform the Director immediately.

A. Oral requests

1. **Library information shall not be released in response to oral requests by law enforcement officers.** The term "library information" includes library business information as well as any patron-specific information. It also includes information in whatever form—whether remembered by employees**,** maintained in paper or electronic files, **or** remaining on public computer workstations. Officers making such requests should be informed of this policy and referred to the Library Director. In all such instances, employees should document the request and contact the Library Director or the person in charge.
2. To the extent that an officer makes an oral request for non-confidential and non-library information (e.g., requests whether a person in a photograph has been in the Library), an employee may, but is not required, to respond. This policy recognizes that, as citizens and library employees, there is an interest in the effective functioning of law enforcement and intelligence agencies and may wish to cooperate. However, the subtle distinctions between confidential and non-confidential information and the ease in which questions may progress to confidential matters suggest caution. If there is any doubt, the Library Director or person in charge, should be consulted.

B. Emergency situations with confidentiality implications

1. Information may come to the attention of an employee—orally, visually, or electronically—that reasonably presents evidence of past, present or future crime. Such information shall be secured immediately and the Library Director or person in charge informed immediately. If such information reasonably suggests an immediate danger of death or serious physical injury, and the Library Director is unavailable, the employee shall contact the person in charge who then may contact the local police.
2. Exigent circumstances may permit law enforcement to enter and seize information and equipment from a library without judicial process. Such rare, warrantless seizures are only appropriate where necessary to prevent the immediate destruction of criminal evidence. If such demands are made, allow the officers to proceed, but follow steps below for search warrant procedures.

C. Written demands by mail or delivery service

1. Written requests in the nature of judicial process (or otherwise requesting information) received by mail or delivery service are forwarded immediately to the Library Director.

D. Written demands presented in person by law enforcement personnel

1. Invite any law enforcement officer (or other individual) presenting judicial process to a private office; (Library Director or person in charge);
    a. Request identification (badge, current law enforcement agency-issued photo identification credential, and a business card);
    b. Record the name, title, agency, and telephone number of the officer, and
    c. Request a copy of the warrant/subpoena and any associated documents.
2. If the document is a **subpoena** or **intercept order** that requires information or action **in the future**, the officer may simply leave a copy;
    a. Inform the officer that only the Library Director is authorized to accept the document and sign for it**;**
    b. Inform the officer that the Library Director will be notified as well as the City Attorney. **Note: Comply with the gag order if a FISA request.** (Only the Library Director may be informed.)
    c. Request the officer's identification; (Note: a badge, a current law enforcement agency-issued photo identification credential, or a business card)
    d. Record the name, title, agency, and telephone number of the officer or individual;
    e. Request a copy of the subpoena and any associated documents;
    f. In all events, the person authorized to and accepting the subpoena should note orally and in writing that "service is accepted in official capacity only."
    f. Document Library costs for complying with the request.
    g. Ask all involved staff not to discuss the matter with the media, family, patrons, or other employees since decisions in this regard must be made by the Library Director.
    h. Complete an incident report form immediately.
3. If the document is a **search warrant**, which authorizes **immediate** search and seizure, the Library must comply with the warrant and instructions of the officer;
    a. Inform the officer that the Library Director and City Attorney must be contacted immediately;
    b. Call the Library Director or designee;
    c. Invite the officer to a private office;
    d. Request to see the credentials of the individual serving the order; (i.e. a badge, a current law enforcement agency-issued photo identification credential, or a business card)
    e. Record the name, title, agency, and telephone number of the officer;

f. Call the office of the individual to verify the credentials;
g. Ask to have the City Attorney present before the search begins (if not a FISA request);
h. Request the patience of the officer;
i. Be polite;
j. Cooperate with the search warrant to ensure only those records in the warrant are produced;
k. Comply with the gag order if a FISA search warrant;
l. Document Library costs for complying with the request.
m. Complete an incident report if not a FISA request.

E. If the terms of the warrant are **"secret" or "sealed"** (issued by the U.S. Foreign Intelligence Surveillance Court or by other courts in particularly sensitive matters), **staff may not disclose any information relating to the warrant or its execution**.
    a. Notify the Library Director.
    b. If a search warrant has been presented and the law enforcement officer will not wait for the Library Director or City Attorney,
    c. Politely remind the officer that the Library is an innocent third party and that Constitutional considerations and good faith suggest that a brief delay is appropriate.
    d. If the officer still declines to delay,
        1) Inspect the warrant carefully;
        2) Monitor the search;
        3) Do not impede or obstruct the search.

F. Monitoring the Search Warrant Execution

1. Keep in mind that computer searches may be executed in four basic ways:
    a. Search the computer and print out a hard copy of particular files at that time (not frequently used because of potential loss of metadata and other information);
    b. Search the computer and make an electronic copy of particular files at that time;
    c. Create a duplicate electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review; and,
    d. Seize the equipment, remove it from the premises, and review its contents off-site.
2. Keep in mind that the option selected depends significantly on the role of the computer hardware in the possible offense;
    a. If the hardware is itself evidence, law enforcement officers usually plan to seize the hardware and search its contents off-site; this is not usually typical of a library environment;

    b. If the hardware is merely a storage device for evidence, officers generally only seize the hardware if less disruptive alternatives are not feasible.
3. Keep in mind that while the Library Director or person in charge may object to actions believed to be in excess of the terms of the warrant, he/she can do nothing to prevent the officers from seizing information deemed appropriate.
4. Undertake the following specific steps:
    a. Enlist the assistance of one other person in the chain of command to work with and accompany you in order to record and remember relevant facts and events;
    b. Ensure that the warrant is signed by a magistrate or judge; Note: National security letters are not signed by a judge or magistrate.
    c. Note exactly what records or items are authorized to be seized; and,
    d. Volunteer to assist the officer by locating the information, enlisting the assistance of those on the staff who are knowledgeable, and offering to provide copies of electronic information in lieu of seizure of hardware; if recordable media is seized, request the opportunity to make copies before it is removed.
    e. Note areas and rooms entered, files and computers inspected, and/or specific actions;
    f. Attempt to make copies of all records seized;
    g. Note and advise the officer if information is being seized that appears to be in excess of that authorized by the warrant;
    h. Note and advise the officer if information being seized that is privileged (e.g. patron specific information, employee records, or attorney/client) and ask that it be so marked.
5. Ask for an inventory of the search at the conclusion of the search; Note: Do not sign any statement that the inventory is accurate or complete; and,
6. **Ask all involved staff not to discuss the matter with the media, patrons, family, or other employees.**