Karen Coyle kcoyle@kcoyle.net March, 2007

SFPL Data Privacy Audit

Introduction

In February and March of 2007, the San Francisco Public Library engaged in an audit of library records that contain data about use of its materials and facilities. In accordance with California State Law[1] the library is obliged to assure confidentiality of records relating to registration and circulation. Although we often commonly refer to this as "patron privacy," the scope is limited to records kept by the library and not to larger issues of personal privacy.

Not all library records are deemed confidential by the relevant laws and policies. Disposition of administrative records is governed by other statutes and policies. In particular, information regarding fines or payments owed by library users is not covered by the confidentiality obligation of the library. Those records are managed under the City of San Francisco records retention rules.

The purpose of the audit is to create an inventory of all library records that fall within the definition of the confidentiality rules, to determine exactly what data is gathered, who has access to the data, and the records retention practice in relation to that data. The inventory is a tool for library management: it brings together in one place the data that the library manages and the current practices around that data. With the inventory in hand, library management can determine whether current policy is supported by the practices, and can make determinations of areas where either policy or practice must be modified.

Background

This is SFPL's first formal data audit. That does not by any means imply that records confidentiality had not been considered before this. The library's privacy policy is evidence that the issue of patron confidentiality has been considered in depth. In most areas the library has strong policies and practices for limiting retention of data and access to records.

The provision of services to individuals necessitates some data collection and use. Although anyone can enter the public library and use materials on site without providing any personal information, borrowing of materials and use of some licensed services requires that the person has been issued a library card. The record of that card identifies the user and provides contact information. Some services require more detailed information than that collected about regular borrowers. For example, the library provides a service to local residents who are housebound. These persons cannot go to the library to select materials to read, so library staff must keep a record representing the person's preference in reading materials, and a list of items they have already read.

The library's obligation is to assure that only the data necessary to perform the service are gathered, and that the record is only kept for as long as is needed to provide the service or to meet any institutional or city-wide records retention rules. In addition, access to the data should be limited to those who must use it in the performance of their library duties.

A comparison of the library's privacy policy with actual practices showed overall consistency. The one area where the policy and practice were not in concert was, ironically, with the general availability of the privacy policy itself. This is reflected in Recommendation 1, below.

---

[1] California Government Code, Section 6267

The Data

The audit looked at records storage in the following areas. These areas were identified by the library's staff as having some data gathering in the course of the provided service:

- Circulation and borrower records
- Library database and system
- Reference services
- Library web site
- Reader services
- Public workstations
- Remote and licensed services
- Meeting room use

Of the data inventoried, the patron database, which contains the library cardholder records and the records that support the circulation of items, is the largest store of patron information. This information is managed within the database software provided by Innovative Interfaces, Inc., a major supplier of library systems. Because most U.S. states have laws that protect the patron data, these systems are in conformance with a U.S. library's need to keep patron information confidential. For example, the information on books checked out is only kept in the patron record until the items are returned, at which point the book data is deleted from the patron record.

There are other products and services used by the library that also are purchased or licensed from vendors accustomed to library practices, including privacy practices. While the library does not have physical control over the actions of online vendors from whom it licenses access to various databases, SFPL does include specific language in its licenses regarding privacy. Through these licenses, and through the privacy policies of the vendors themselves, the library obtains assurance that personally identifiable patron data will not be used for purposes other than providing the licensed services.

There are services provided by the library that are part of state or national programs, and these programs determine the data to be gathered and also the retention rules. An example of this is the library's participation in the National Library for the Blind. With these services the library has an obligation to inform users of the data being gathered and the agency that is responsible for securing that data.

In some areas the library develops its own programs and therefore is the sole agency responsible for the data gathering and management. This is especially true in the area of reader services, where both the main library and branches run programs for children and adults that encourage reading. These programs vary in their formality, with some being on a drop-in basis that do not keep any records, to others that require signups and issue raffle tickets for prizes. For these programs, which can vary from branch to branch, there is a tendency for programs to manage their data in an ad hoc manner. Some librarians at SFPL are also beginning to use non-traditional communication methods to contact patrons about programs, such as e-mail, instant messaging, and social networks like MySpace. These communication methods will reach new generations of library users and should be included in the library's consideration for privacy of communications with patrons.

Recommendations

The SFPL management will review the audit inventory to identify any areas where data practices need attention. The resulting tasks will be prioritized for implementation. The list of recommendations below gives some general direction toward library actions, but is not to be considered a substitute for the tasks that will be developed by the library in its analysis.

These are general, and the library will be looking at these and specific may develop more specific tasks based on these.

1. Make the library's privacy policy more visible to users. Link to the privacy policy from each web page on the library's site, and create a pleasing brochure that library visitors can pick up and take with them.
2. Develop general policies for data gathering and data retention for ad hoc activities, such as informal reading groups. These policies should not try to address every specific situation but should provide guidance that can be applied by librarians in a variety of cases.
3. Pay particular attention to data that identifies under-aged patrons or other special populations. Where sensitive information is required for the provision of a service, such as service to library users with disabilities, develop policies for secure storage of paper or digital records.
4. Using the data inventory, identify any areas where library procedures are not in compliance with the stated policy, such as records retention rules.
5. Develop a definition of "lapsed library card holders" so that those entries can be purged from the patron database.
6. Develop a plan for continuing education of library staff in the area of records confidentiality. If possible, include training on the handling of law enforcement requests for data.
7. Pay attention as the library embraces new channels of communication with patrons, such as instant message and social networking (e.g. MySpace). At an appropriate point develop policies for these activities that will address patron confidentiality issues.
8. Name one or more "privacy officers" among library staff. The role of these persons will be to:
    a. keep themselves informed about developments in the area of privacy as it affects the library
    b. be the focal point(s) for questions about library practices relating to privacy and records confidentiality
    c. take responsibility for the ongoing management of staff training
    d. manage periodic review of the privacy policy and future audits