FEATURE

Train Employees and Officials to Be Ready for Privacy Challenges

Vol. 27 No. 6 — June 2007

by Joen E. Bernstein

Don't find out the hard way that you and your staff do not know how to respond when the police come knocking on your door in search of information that's contained in your library's customer records. You may believe that you are prepared, but unless you have thoroughly addressed this issue with your staff and have done structured training that's been repeated over time, you may find yourself in an awkward position that could create havoc in your library. When I think back to what happened in my library 2 years ago, and as I compare notes with colleagues who have also been approached by the police, I realize that you can never overestimate the need for preparation and planning to be ready to deal with authorities when they're in search of someone's confidential library data.

In 2005, I thought my people at the Mount Laurel (N.J.) Library were in fairly good shape in terms of the professional staff's understanding of the confidentiality rules governing our customer information. But I was wrong. This was driven home by a series of events—thankfully, unusual ones—that occurred that spring.

Behavior Raised Suspicions

Over the course of a few months, a particular library user had caught the eye of some of our staff members. His actions made the staff curious and suspicious of him. He would spend time at a public computer and then rush to our public printer to grab his print jobs. A couple of times, staffers saw him stuffing the printouts into his shirt. We talked about this and decided there was no basis for action on our part, since the user was not disruptive, and there had never been an incident of anyone who was using nearby computers complaining about his behavior. Several months passed. The man came in frequently, and his behavior was always the same.

One day, a member of the professional staff could no longer resist his curiosity and managed to catch a glimpse of some of the pages the man had viewed. The staffer, very upset by what he had seen, called me out of my office to show me several pictures of little boys in bathing suits. Obviously, this struck both of us as weird and more than a little creepy, but I advised the staff member that, while the behavior made us uncomfortable, viewing pictures of little boys in bathing suits was not illegal and it would be a stretch to call those pictures pornographic, although the staff member had characterized them as such. We agreed that we would keep an eye on the customer to see if his behavior became disruptive or if his actions were inappropriate in any way.

One day not long after, this same staff member was covering the information desk. He needed to clear a jam in the queue of one of our public printers. He noticed that the man was again in the computer lab printing out more pictures. This time the man left the library before picking up his print job. The staff member made note of the man's library card number from the records in the print queue log and subsequently checked the system in order to determine his name and address.

It is often the case that excitement in the library seems to occur on evenings or weekends when senior staff members are less likely to be in the building. However, it must have been particularly quiet one Saturday, because I received a call at home from this same staff member informing me that he had taken the liberty of searching the New Jersey Sex Offender Registry for the customer. It turned out that he was listed. When I spoke to the staff member, he was very agitated by his findings and thought we should call the police. I determined that the man had not even been in the library that weekend, so it was certainly not a situation that required emergency action. Moreover, because of the underlying issues, I told him to take no action until we could fully discuss it on Monday morning.

The Critical Decision and Its Consequences

Unfortunately, the staff member was so upset that he made the decision to call the police that day. The police immediately came to the library, asked to speak to the librarian who had contacted them, and asked him to point out which computers the man had been using. It was fortunate that the staff member pointed out only two computers, because the police promptly seized both and removed them from the library. When the employee asked the police whether they needed a subpoena to take library property, the police explained that the public library is part of the municipality and, therefore, none was needed. He accepted their explanation, and the police left with the computers. You can imagine my delight when I heard about all this later in the weekend!

After 2 months of "investigation," the police concluded that no crime had been committed, and they dropped the matter and returned the computers. However, in the interim, we received numerous visits from the police, and we spent many hours talking with policemen, attorneys, and library staff, generally trying to manage a problem that had spun out of control. One detective threatened to have someone come to the library and search our servers, although he indicated no particular objective for the search. Another detective continued to pressure me to turn over the pictures of little boys in bathing suits that the librarian had found in the public printer. When, during a meeting with him, I refused to give him the pictures without a subpoena, the detective produced a subpoena that he'd had with him the entire time. Apparently, he was testing me to determine if I would "cooperate" or insist on being "difficult."

Although the event ended without legal action, it left a legacy. Many of the parties involved bore scars in the form of lasting hard feelings and disruptions to important work relationships. Reflecting back some 2 years later, I think that there were several key lessons to be learned from the experience. The lessons relate to library customer information contained in automated records and to personal beliefs, human emotions, and motivations.

Emotion Versus Training

First, the staff member who took it upon himself to call the police continued to believe that he had behaved properly in his proactive attempt to stop a sexual predator, and that I was wrong in feeling otherwise. He actually left his position some months later, and although he did not cite these events as the cause, I think they may have played a part. The police believed that I was being an obstructionist and continued to harbor a negative view of the library long afterward, even though I explained that the library's position was based not in an unwillingness to help, but rather in our state's laws. The New Jersey laws that govern library customer information prohibit me from surrendering customer records without a subpoena. This explanation seemed to fall on deaf ears, and we were treated as if we were deliberately hampering their investigation.

Second, emotions play a large part in how these issues play out. Staff members are, after all, people too. They will fear people who might do harm even if those people are not acting in a disruptive manner in the library. In our case, the emotional reaction was to an individual who was a potential sexual predator, but you can easily substitute an alleged terrorist, a bank robber, a homeless person, or even a political dissident. Fear is an emotion that can motivate staffers to respond inappropriately, especially if they are not adequately trained to deal with these issues. The police have a mandate that is fundamentally different from ours as librarians, and they may react emotionally, with hostility and even outrage, when our actions force them to recognize those differences.

You should take nothing for granted when it comes to preparing your staff to perform appropriately as protectors of customer privacy and confidentiality. If you want your staff to know something, make sure you communicate it to them, in many ways and many times. When you are absolutely sure they have internalized the message, communicate it again! Remember that this stuff is emotion-laden, and the emotional content of an encounter will be stronger than the professional training unless the latter is truly internalized. Especially because the precipitating event will almost certainly come up suddenly and unexpectedly, it is essential that staff know precisely what their responsibilities and obligations are. My staff member's fear over having a convicted sex offender in the library took precedence over his professional responsibility of preserving the man's privacy. Fear trumped his ability to perform his job appropriately.

Who Needs to Know What

What's a library director to do? First, acknowledge what ripple effect this may have on your institution. The issue of privacy of automated library records affects everyone from pages and patrons to the library board of trustees and township officials. You need to make sure that you reach out to all groups so everyone understands the issues and our professional responses.

Let's take a look at each of these groups:

First, library directors need to educate themselves on the laws protecting the confidentiality of library customers. The laws are complex and there is potential inconsistency between local ordinances, state laws, and federal laws. Assistance from an attorney who has direct involvement in First Amendment issues is exceedingly useful in this effort. Once you understand the legal issues, you and the board of trustees (or other similarly functioning body) must develop, approve, and put in place a privacy policy, making sure that it is in compliance with the current laws. Following that, clear and consistent procedures must be developed, ideally with extensive input from library staff, to implement this policy.

Every staff member must be trained so that he or she knows what procedures to follow if the police should request confidential library records from them. This training should include

some background information about the Bill of Rights, the USA PATRIOT Act, state privacy protection laws, etc., so it is clear to them that there are legal underpinnings for the policy they are expected to implement. This will go a long way toward addressing any personal conflicts that staff members may have with implementing policies. They need to understand that we're not doing this on a whim, but rather because the law dictates we do so.

Members of the public need to be educated about their right to privacy regarding their library records. I have observed that many library customers are surprised to learn that we are so protective of their library use records but most seem appreciative that we are. Informing them in the information flier you give them when they receive a new library card is a good way to communicate this.

The police need to be educated in library law. You should meet with your local police chief and talk over your privacy policy and procedures so they will know what they need to bring with them should they ever need customer records for an investigation. You might offer to develop training materials or presentations for police officers. It's a good idea to explain to the police chief and to all police officers that respecting the confidentiality of electronic library records and obtaining the required legal approvals before requesting those records will speed their investigations and will help them make charges stick if they decide to prosecute. Evidence that's gained in violation of due process will eventually face challenge in court, and an otherwise strong case may fail because of it.

Your municipal or institutional officials need to be kept in the loop as well. While they may not become directly involved in any issue that might arise, they need to know how your library will deal with it. Giving them the opportunity for buy-in is better done before any issues arise, when emotions are not inflamed, and when public pronouncements have not been made. There is nothing a politician or executive dislikes more than a surprise, except perhaps for an embarrassment.

Retaining Your Records

Record retention is another issue that we, as managers of confidential library information, must address. You should definitely have a documented record-retention policy that covers all library data. A policy addressing the disposition of both paper and electronic data should describe what records your library retains and for what length of time. A good rule of thumb is that the less you retain, the less you have to worry about. You should not retain any records that you do not need to retain for the effective and efficient operation of the library. There is absolutely nothing illegal or unethical about destroying or deleting records in a manner that is consistent with an established and documented record-retention policy. However, unscheduled deletion of records in anticipation of, or worse yet *after*, being served with a subpoena, very definitely *is* illegal. I've heard of some libraries that retain copious amounts of users' records in the belief that this will help the police, should they ever need the information for an investigation. Unfortunately, the record gathering could very well reveal others' records as well as those of the individual the police are investigating. Is that really the best way to preserve our users' privacy? I don't think so.

The browser history files in public computers and in the sign-up sheets customers use to reserve them are two more spots where our public's privacy can be compromised. The browser history, which shows all of the Web sites users have visited, can be set to delete every time a computer is rebooted or it can be set so that no history is retained at all. There is no valid library management reason to retain browser history files, so they should be deleted, both for confidentiality reasons as well as for simply good computer maintenance. Similarly, sign-up sheets can be shredded at day's end. If they are needed for statistics, staff can collect the statistics promptly and then shred the papers.

In my library, all of our public computers are networked with a central print server. In order for users to retrieve their print jobs, the software links the job to the user's library card number. While the public does not have access to the history in the print server, it does exist until the information is deleted. So here is another access point for gathering information on users that you need to address.

Prepare to Protect Patrons

Being prepared takes time and effort. As I previously mentioned, there are a number of groups that need to be educated and enlightened, and they all play a key role in protecting your customers' privacy rights. But the library staff members are most important. They are the ones who carry out our procedures and enforce our rules. They need frequent reviews of these policies and procedures to ensure that they will act confidently if they are approached by law enforcement officials seeking confidential library records.

Anyone who has been involved in such a situation can tell you that the time they've invested in ensuring that their library is prepared was well worth it. It's part of our responsibility as professional librarians, and our library users deserve nothing less.

Joan E. Bernstein *is the director of the Mount Laurel (N.J.) Library and the president of the New Jersey Library Association (NJLA). She holds an M.S. from the Drexel University College of Information Science and Technology in Philadelphia. She is a member of NJLA's Intellectual Freedom Committee, which developed guidelines to assist libraries with requests for confidential library records. She selected Protecting Privacy and Freedom in Your Library as the theme for her NJLA presidential year. Her email address is* ***jeb@mtlaurel.lib.nj.us****.*