Are Libraries Compromising Reader Privacy with Circulation Reminders?

By Robert P. Holley

A faculty member asked me about reader privacy during a recent meeting. I reassured her that most libraries erase circulation records as soon as the items were returned, that state law protects the privacy of library records, and that libraries in general are doing all they can to make sure that others will not be able to discover what their patrons read. I then suddenly stopped short. A new library service may be undoing all these attempts to protect reader privacy. The e-mail circulation reminders that both my academic and public libraries send me include my name and a record of the books that I've checked out. The libraries send these reminders out unencrypted. They get passed through all sorts of transit points on the way to me. They then sit in my e-mail box until I get around to deleting them. Furthermore, my e-mail provider may have cached copies of these e-mails, perhaps in multiple locations, as part of routine backups and other housekeeping duties. I also have my personal backup copies on a flash drive that would become available if anyone stole my briefcase.

I am bringing this issue up because I have not seen any discussion of this reader privacy concern though I cannot be certain that none exists. I am also not a lawyer so that I am giving a layman's interpretation of the laws surrounding library record confidentiality and could be wrong. I would welcome having those with more legal expertise address the status of circulation reminders in comparison with internal library circulation records.

The nature of e-mail itself provides the first possibility for the violation of reader privacy. To give some documentation on this issue, I'll quote three short sections from an article on e-mail security to show just how unprotected e-mail is from prying eyes.

> You may already know that e-mail is insecure; however, it may surprise you to learn just how insecure it really is. For example, did you know that messages which you thought were deleted years ago may be sitting on servers half-way around the world? Or that your messages can be read and modified in transit, even before they reach their destination? Or even that the username and password that you use to login to your e-mail servers can be stolen and used by hackers?

Eavesdropping: The Internet is a big place with a lot of people on it. It is very easy for someone who has access to the computers or networks through which your information is traveling to capture this information and read it. Just like someone in the next room listening in on your phone conversation, people using computers "near" the path your e-mail takes through the Internet can potentially read and copy your messages!

Unprotected Backups: Messages are stored in plain text on all SMTP Servers. Thus, backups of these servers' disks contain plain text copies of your messages. As backups can be kept for years and can be read by anyone with access to them, your messages could still be exposed in insecure places even after you think that all copies have been "deleted" (Case, 2009).

All the efforts within the library to protect reader privacy are thus undone by the circulation notice that puts the information about my reading habits in an insecure environment. Anyone with access to the e-mail backups can easily find out what I've checked out by using my name and the name of the library as keywords to access the files. I may think that I don't need to worry, but perhaps I've made an enemy in the IT division of my university on account of the critical comment that I posted on a national blog. Perhaps the faculty member who asked me about the security of circulation records has an ex-spouse or ex-significant other who wishes to snoop. Would the library send out such a reminder with detailed information on the books that I've checked out on a postcard, visible for all to see? Yet one of the analogies that I've heard for years is that "e-mail is like a postcard."

The second set of threats comes after the circulation reminder is delivered to my computer. I get the reminder e-mail for books checked out from the Wayne State University Library System on my work computer because the library uses the e-mail addresses provided by the university. While a recent court decision has ruled that some e-mails sent or received at work are private, this decision is not broad enough to reverse the generally accepted principle that employers can read e-mails on an employee's computer (Fisher & Phillips

LLP, 2010). While doing so may actually be against a strict interpretation of my employer's e-mail policy, I also receive my public library's circulation reminders at work.

I may also need to worry that malware has infected my computer. "Today, authorities believe that there are between 20-40 million infected computers in the United States alone" (Password , 2006). While the attackers are most likely trying to discover the password to my bank account, their efforts, including examining my files and logging my keystrokes, could compromise the security of any records stored on my computer. Techniques also exist to steal my e-mail passwords allowing hackers to access my e-mail account wherever my e-mails exist in the cloud. Furthermore, today's e-mail providers allot almost unlimited storage and discourage users from deleting e-mails.

I'm a cautious computer user and make backups of my e-mails. I carry these backups on a flash drive in my briefcase. If someone were to steal this flash drive, this person would be able to recover my e-mails with the library circulation records.

While others exist, the last illegal threat to my library records that I'll note is hacking my e-mail provider. Both the University of California-Davis and Yale University have decided not to use Gmail on account of "potential problems with cloud computing" (Schools, 2010). While the theft or loss of data has not usually been associated with e-mail, the possibility is real.

Libraries also seek to protect patron circulation records from government scrutiny. Law enforcement officials have been known to ask employees at library service desks to supply circulation records even if doing so may be illegal without a court order. While staff in libraries have generally been trained to say no to such requests, the same may not be true for the IT person if the police officer shows up at a time when higher level supervisors are not available and the officer flashes a badge with a request to retrieve e-mails from the backup tapes.

While the laws protecting the privacy of library records vary from state to state, I would guess that many of these laws do not give e-mail circulation reminders the same higher legal protection that circulation records have. First, the library has sent out these reminders with the knowledge that e-mail is not a secure medium. Second, unless the laws have been updated recently, e-mail may not have existed when the various states enacted privacy statutes on the confidentiality of library records. In fact, law enforcement officials may not be specifically looking for library records when using a subpoena for e-mail records. I am not a lawyer so that the confidentiality laws may apply to circulation reminders, but I would not count on this without having a court case to support this position.

Access to e-mails is also not necessarily limited to government officials but may occur with civil actions. The following is the Google policy: "As stated in our [Terms of Service](#) and [Privacy Policy](#), Google complies with valid legal processes seeking account information, such as search warrants, court orders, or subpoenas" (Google). Fortunately, while a person's entire search history is available for the asking by subpoena, "that type of fishing expedition is not legally permitted for Web mail providers" since e-mail is shielded by the 1986 Electronic Communications Privacy Act (McCullagh). A subpoena asking for e-mail on a specific topic might be legal. The legal process called discovery often requires providing e-mail records that might include circulation reminders. A review of various news stories on access to e-mail by subpoena indicates an unsettled area of the law with contradictory court decisions.

If the concerns that I have expressed above have any validity, what should happen next? My principal suggestion is to explain the issue to library users and let them opt out of receiving e-mail circulation reminders if they have concerns about their reader privacy. Public libraries should find it relatively easy to implement such a policy since they have to ask their patrons for their e-mail addresses. The public library might even have a short form for patrons to sign when providing their e-mail addresses. As with most privacy agreements, I would bet that most will sign the form without bothering to read it. The case of academic libraries with automatic access to their patrons' e-mail addresses is more complicated. Perhaps each reminder could include a short statement about the potential privacy concerns and include an opt-out link similar to those that are included in many advertising messages. This link, however, must be operational unlike the ones from many spammers whose only goal is to verify the e-mail address for next time.

Perhaps some might consider my concerns to be alarmist. "Protecting user privacy and confidentiality is necessary for intellectual freedom and fundamental to the ethics and practice of librarianship." This statement appears on the American Library Association website that gives the "Core Values of Librarianship" (American, 2010). Efforts both legal and illegal to obtain access to circulation records may not occur all that frequently; but, when they occur, librarians have frequently pushed back as hard as they could, often against public opinion. In fact, librarians have considered protecting reader privacy important enough to do battle with the FBI and the Justice Department. The proverb states that "the chain is only as strong as its weakest link." With all the vigilance to protect circulation records within the library, I worry that libraries have created a weak link by sending out e-mail circulation reminders that will make it easier to learn what their patrons read.