Smart Libraries Newsletter

News and Analysis in Library Technology Developments

ALA TechSource
alatechsource.org

225 N Michigan Ave, Suite 1300, Chicago, Illinois 60601, USA

Smarter Libraries through Technology

Privacy and Security in Times of Crisis

By Marshall Breeding

I have written frequently on topics related to the responsibility of libraries to safeguard the privacy of their patrons, both in their physical lending operations and their digital services. It is a core value of the profession. In this time of a global health crisis, I see it as important for libraries to continue upholding privacy protection.

One of the important elements of controlling the spread of the coronavirus involves contact tracing. If a person becomes ill with, or tests positive for, COVID-19, to limit further spread, it is important to determine the other persons who may have been exposed. As noted in a recent *American Libraries* article,[1] the skills of librarians are well suited to this task, especially since they bring a concern for protecting privacy to the process. I would further emphasize the need for a strong firewall between any patron data in library systems and involvement by library personnel in contact tracing. The use of names and addresses in patron records for other purposes, even for a good cause such as public health, would probably be inconsistent with most library privacy policies. The use of ILS contact details to make calls to check up on elderly or vulnerable patrons may likewise exceed the terms of privacy policies.

As libraries and other organization begin to reopen their physical facilities, they often do so with restrictions specified by local or state agencies or by their own guidelines for ensuring social distancing. There may be, for example, restrictions on occupancy to specific numbers of individuals or to a percentage of normal occupancy patterns. There may be ways to use technology to manage the flow of visitors to library facilities. The obvious concern here is that technology used to monitor and control building occupancy does not capture personal data or at least treats that data with the same degree of security and protection applied to circulation records. Data regarding the physical presence of an individual in the library may be even more sensitive than records regarding patron use of library collection materials.

Many organizations are implementing procedures to monitor the health of their employees, such as daily temperature checks. To the extent that libraries perform these kinds of procedures, care should be taken in where any of this information is recorded. The management of health-related data comes with an different set of regulatory frameworks than most library systems are designed to accommodate.

Though not necessarily related to library technologies, concerns about the use of facial recognition have heightened in recent weeks. Top technology companies, such as IBM and Microsoft, recently made announcements that they will cease, or at least pause, the development or investment in facial recognition technology due to concerns for privacy. As facial recognition technology becomes ever more accurate, widely deployed, and tied to large scale repositories of personal data, the implications for broad surveillance or other intrusions into personal privacy raise serious societal concerns.

Concerns specific to the library context have also arisen. With the advancements of facial recognition, we must assume

IN THIS ISSUE

Libraries Prepare to Reopen
PAGE 2

Overdrive Sale Has Closed
PAGE 4

Smart Libraries Q&A
PAGE 4

Notes
PAGE 7

ISSN 1541-8820 July 2020 Volume XL Number 7

that any video that includes people should be considered a source of personally identifiable data. Video from security cameras, for example, in conjunction with facial recognition systems represent records of when specific individuals were physically present in the library. Again, libraries should treat this video according to their policies for patron privacy protection.

While libraries adopt their own institutional privacy policies, a set of basic technical principles are needed to support them. These include authenticated access to any personally identifiable information (PII), restricting it to the roles of personnel requiring its operational use, encryption of any PII storied on library systems, and end-to-end encryption of all personal data as it traverses local networks or the internet. Personal information would also include data associating individuals with physical or electronic library resources borrowed, consulted, or viewed. Other technical measures related to privacy include anonymization of transactions related to the use of materials and automated routines to execute data retention policies. Libraries and their system vendors must also be sure to keep up-to-date with encryption technologies. Standards continually change based on discoveries of new vulnerabilities.

Libraries need a strong firewall between patron data in library systems and involvement in contact tracing.

The protection of patron privacy requires constant vigilance. New advancements in technologies may come with inherent implications related to privacy and security, some of which may not be immediately apparent. Any time that a library expands its involvement into new areas or implements technology for new patterns of service, there should be careful attention to any possible collection and retention of personally identifiable information. Products developed for the consumer or business sectors tend to be quite aggressive in the capture and use of such data. Maintaining a technical environment able to fully support the values of the library profession as well as the policies of individual libraries requires continual effort. Technical standards constantly change, and the consumer and business sectors have shown an ever increasing appetite for personal data.

Libraries Prepare to Reopen

Although the COVID-19 pandemic crisis has not yet fully abated in the United States, most states have begun a process of reopening, allowing businesses and other organizations to resume public activities with varying levels of restrictions. Libraries are part of this movement, striving to provide services to their communities in ways that assure the safety of library workers and their patrons.

During the crisis libraries have put great effort into their digital services. Even though physical branches may have closed, libraries have looked to creative ways to fulfilling their roles. Most public and academic libraries have remained very active in promoting and operating their digital services, especially ebook lending, enhanced access to other electronic resources, remote reference, or virtual programs.

In the current environment many questions remain without definitive resolution, such as how long the coronavirus remains on materials and how easily it can be spread in indoor and outdoor settings. These unresolved questions lead to uncertainties in procedures that libraries might follow to safely resume services. In the interim, many libraries are working to identify a subset of services to enable at least some level of access to physical collection materials.

IFLA is monitoring responses to the COVID-19 pandemic by libraries in many global regions and countries. The organization recently released an overview of how libraries in 30 different countries are approaching the crisis.[2]

REALM Project

OCLC, the Institute of Museum and Library Services (IMLS), and Battelle are collaborating on REALM (Reopening Archives, Libraries, and Museums) project. This project will produce a toolkit of resources to assist organizations in developing procedures and strategies for reopening their facilities and services during the COVID-19 crisis. This project will select, collect, and disseminate existing relevant resources during its first phase (May – August 2020).

Phase One of the project also includes laboratory testing that will be conducted by Battelle to investigate key issues such as how long the coronavirus persists on collection materials.

The materials to be tested include hardcover book covers, buckram book covers, paperback book covers, internal book pages, plastic protective book covers, and plastic DVD cases. Battelle has issued the document "Test Plan for the Natural Attenuation of SARS-CoV-2 as a Decontamination Approach," which describes the methodology that it will follow in its laboratory research. The document includes a statement of the objective of the research project:

> The overall objective of this project is to gather data for OCLC and IMLS on the efficacy of ambient environmental conditions (temperature and relative humidity [RH]) against SARS-CoV2 pathogenic virus applied to representative materials found in libraries, archives and museums. OCLC and IMLS will select the materials and number of organisms to be tested, and Battelle will obtain and experiment with the agents.[3]

Battelle's laboratory research will provide important information regarding the persistence of the virus on collection materials. According to the timetables outlined in the REALM project website, the research will be carried out during the phase that concludes in August 2020. Since many libraries have reopening activities underway as of the beginning of June 2020, they will need to rely on more general research on the potential risks involved, rather than this specific research on library materials. Once the project's results are published, libraries will be able to make any needed adjustments to their procedures.

Subsequent phases of the project will study additional types of materials and address issues not resolved in the earlier phases, producing additional resources for the toolkit. The project will remain active through September 2021 and will monitor any new research relevant to the stakeholders, updating toolkit resources as needed. The project description notes that "as the rate of transmission for the virus changes over time and communities continue to adjust to those changes, the policies and practices of libraries and museums may also warrant a change."[4]

Battelle's laboratory research will provide important information regarding the persistence of the virus on collection materials.

Selected Vendor Responses

All the ILS vendors are working with their customers through formal and informal channels to provide assistance in configuring or customizing products as needed to adjust to new workflows and procedure. Several library technology vendors have announced products or services to assist libraries as they implement reopening activities.

Patron Point Helps Libraries in Messaging

Patron Point announced that its customers have been able to use its automated messaging environment to facilitate reengagement with community members and to measure results. The system is able to identify patrons that have not been active in recent months and promote digital services such as ebooks and virtual programs. Patron Point can generate sequences of messages promoting relevant services to new or re-engaged lapsed-patrons. Patron Point offers a number of options for managing circulation notices. It can be programmed to customize the text of pickup messages. Libraries can schedule pickup notifications according to any necessary quarantine delays, allowing staff to avoid handling materials for specified intervals. Patron Point also selectively filters the generation of pickup messages for facilities that remain closed.

Curbside Feature for Evergreen

One of the common procedures implemented by libraries involves setting aside any returned materials for a specified interval before they are handled by library workers for check-in or processing. This quarantine period is typically set for three days, which studies show is the period that the virus can survive on surfaces.

Many libraries have implemented curbside service where patrons select materials they want to borrow through the online catalog and pick them up in their cars without the need for personal contact. This style of service has become popular for grocery and retail outlets.

New features for the open source Evergreen ILS are underway to support curbside pickup. This capability is being developed by the Equinox Open Library Initiative, sponsored by the Pennsylvania Integrated Library System consortium. The curbside pickup workflow will enable patrons to select materials in the catalog, place desired items on hold, and specify a time for pickup, and finally notify the library once they are on site. Staff functionality includes new displays for holds scheduled for pickup, the ability to view or modify pickup times, and real-time notifications upon patron arrival for materials.

Baratz Creates Features for Quarantined Materials

AbsysNet 2.2.5 from Baratz, includes several new features to help library workers manage items in quarantine. These

include the capability to automatically set the status of returned items to "Temporarily out of Circulation" and to reset materials to active status once the specified quarantine interval expires. This Q-Quarantine feature can be configured by the library, with customized delay intervals and policies regarding the locations and materials for which it will be invoked.

Biblionix Creates Tools for Apollo

Biblionix has rolled out 18 new features for its Apollo ILS for smaller public libraries, facilitating changes in procedures related to the COVID-19 crisis. Apollo's catalog supports patron self-checkout, enabling patrons to sign in and charge materials to themselves using the camera on their phone. Since the Apollo catalog is already fully responsive, no special mobile app is needed. Other self-service features include online self-registration, or in-library signup using a dedicated kiosk. Libraries using Apollo can also opt to boost the placement of electronic items in search results since physical materials may not be available. Apollo also enables libraries to manage due dates, holds, or patron expirations in bulk to accommodate library closures.

Soutron Redirects Resources to its Clients

Soutron Global, which serves mostly legal and corporate libraries, has responded to its current or potential clients facing the financial impact of the COVID-19 crisis by offering discounted pricing for its ILS products and free access to its Discovery platform through the end of the year. Its clients can apply for these programs via its website.

Overdrive Sale Has Closed

The February 2020 issue of *Smart Library Newsletter* featured the proposed transfer of ownership of OverDrive from Rakuten to investment firm KKR. This transaction, initiated in December 2019, closed in early June 2020.

With the acquisition completed, OverDrive is now under common ownership with RBmedia, one of the largest providers to audiobooks to libraries. RBmedia continues to expand its presence in this niche, most recently through its March 2020 acquisition of GraphicAudio, a producer of dramatic audio performances. Any new synergies, partnerships, or consolidation between OverDrive and RBmedia will bring a new dynamic to the library digital content arena. The common ownership sparks interest in such a possibility. However, there have been no public announcements regarding any new relationships, and the two companies remain independent and competitive with each other.

Smart Libraries Q&A

Each issue Marshall Breeding responds to questions submitted by readers. Email questions to Patrick Hogan, Managing Editor, at phogan@ala.org.

What are some of the email transmission standards and protocols that a library should implement to ensure privacy and reliable delivery? Can libraries depend on reliable email delivery for important communications such as circulation notices? How does email fit into marketing campaigns?

Although a mainstay for personal and professional communications, email has also become notorious for its many problems and complications. Since email persists as libraries' primary channel of communications with their users, it is important to be aware of the technical issues and trends in the way it is used.

The number of email messages sent via the internet is massive and continues to grow. An estimated 293.6 billion email messages were transmitted in 2019.[5] Not all email messages involve intentional or wanted use: spam email represents over 55 percent of email traffic.[6] The frustrations of email and the convenience of interactive messaging apps such as SMS (short message service), iMessage, WhatsApp, Facebook Messenger, and others have come to replace email for many types of personal communication. Slack, Microsoft Teams, and IRC have seen ever increasing use for workplace communications.

These use patterns have implications for the way that libraries communicate with their patrons. While almost all

library patrons may have one or more email addresses, they may not necessarily check email regularly. Almost any integrated library system can be configured to also send notices via SMS. Patrons may be reluctant to opt to receive notices this way, possibly out of concern that they will be overloaded with spam via their mobile phones like they experience on their email accounts. Even if a portion of messages can be offloaded to SMS, email will likely continue as the primary way that libraries send messages to their patrons for the foreseeable future.

The main questions with email concern trust and reliability. How do you know that the message is from its stated sender? Is the message sent and received intact, or has it been intercepted and altered in transit? Is the message private, or can others intercept and read it? Does the message contain meaningful content, or has it been generated through bulk advertising? Does it contain malware or link to a malicious site with malware? Is it a message that tempts the receiver to divulge personal information or to fall prey to some type of scam? Many attacks rely on social engineering to take advantage of naive victims. All these scenarios are so common that they diminish trust in email as a communications medium.

Fortunately, the email ecosystem has evolved to provide multiple layers of protection for each of these possible types of misuse. To be considered trustworthy, mail services must implement a complex set of protocols and standards that validate the identity of the sender, the integrity of the message, and guard against most patterns of unwanted or dangerous solicitations.

Gmail, Microsoft Outlook and Exchange, Yahoo Mail, and other major providers of email services have implemented sophisticated infrastructure based on the latest security practices and protocols to safely send and receive messages. Major mail services pass each message through sophisticated algorithms to categorize them according to risk level, automatically rejecting those that fall into obvious categories of unwanted mail and flagging those deemed suspicious. These services offer an option to automatically place suspicious messages into something like a "Junk Email" or to automatically delete them.

The Apache SpamAssasin, a widely implemented open source application for mail filtering, evaluates a complex list of factors to assign each message a score representing the likelihood that it is spam (see: https://spamassassin.apache.org). Errors in technical implementation of mail delivery, suspicious patterns of content, or an origination from a source known to be associated with spam generation result in scores that may fall below the mail service's threshold for trustworthiness.

There are circumstances where libraries need to generate messages to their users or community members. Notices from the library's integrated library system are the classic example. Other scenarios include messages related to event registration, program announcements, or general marketing and publicity. The applications that generate these messages must be configured to format and transmit email messages in strict conformance to the applicable standards and protocols and to follow practices that will ensure their classification as safe for delivery and not rejected as spam.

A number of standards and protocols are involved in the secure and reliable transmission of email messages. Though a bit technical, it is important to have at least a general understanding of the email ecosystem when implementing or evaluating products that involve the generation of email messages to patrons or community members.

In order to generate an email message, the application needs access to a Message Transfer Agent (MTA) that uses the SMTP protocol to transfer the message to the intended recipient(s). Examples of MTAs include Sendmail in the Unix environment or Exchange on Microsoft Windows servers. SMTP uses a series of conversational directives where the application provides mandatory header fields (to: from: subject: date), optional supplemental fields, and the body of the message. It is essential to control access to the MTA by requiring some type of strong authentication before initiating a SMTP sequence. Failure to do so results in an "open relay," which enables unauthorized agents to generate mail via the institution's domain.

Sender Policy Framework

SPF, or the Sender Policy Framework, describes a set of configuration practices that confirm that the MTA is authorized to deliver email on behalf of the domain name representing the organization. This framework includes entries in the DNS (Domain Name System) configuration for that domain. Since DNS configuration details are strictly controlled and can only be made by authorized domain administrators, these configuration entries can be considered as trustworthy. Basic configuration details related to email include the creation of an MX record specifying the mail server authorized for the domain and a PTR entry that enables a reverse DNS lookup, which is useful to email validation. SPF goes beyond these basic DNS entries and involves the creation of a TXT entry in the DNS record for the domain that lists the IP addresses or domains of the authorized MTAs. Receiving mail systems will perform a DNS lookup that validates that the MTA that originated the message properly appears in a TXT entry for that domain. (Example: librarytechnology.org. 37 IN TXT "v=spf1 ip4:xx.xx.xx.xx). SPF

provides a basic level of assurance that the email agent that generated the message is authorized to do so, but does not address every possibility for abuse.

DomainKeys Identified Mail

DKIM, or DomainKeys Identified Mail, provides an additional layer of features that ensure the integrity of the message. It addresses the concern that the message received has not been modified in any way from its original form. DKIM accomplishes this validation via encryption technologies involving public and private key. The application generating the email message produces multiple cryptographic signatures that can be used to validate the integrity of the delivery headers and the body of the message. Hashes are generated using the private key, which is never shared publicly. The DKIM routines then insert an additional header into the message, which is used by the receiver to validate the message. Validation of a cryptographic hash requires access to the public key, which is published in the DNS entry in the sender's domain record in a TXT entry.

Example of a dkim TXT entry:

> dkim._domainkey.librarytechnology.org v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvP/zFa1IAR3HZM6i44ksmvvxOrBMztncbYiqPXWnNljRoOg6x2CMwZPVaODsETpAfSlDff42j0tkP2ZQ0SYNJu6bGlKFKJSvsp+g6FAcnslw3SSN6lDLATQS4zsjLTiZeS/WfsjRMcxL67usCuH80/fyBnt0piTnbOx5QmQpAittwGzctm6ICkHPB8h6oXiVjaab8XBRStOrhDUe76ILVkDr0ppIlqhkf404mSOsowLfU6c5RDmcrYh5xij1sxS/apR/gzSdd4hSuaoIMeeVX4+DHllsYLuPO4AsbkHVqn0djYIL6+rh/q70CYvID6ZI40flhvLjQ8QRmeUAGc3TwwIDAQAB;

Example of a DKIM signature provided in a message header

> DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=librarytechnology.org; h=to:from:subject:date:mime-version:content-type:content-transfer-encoding; s=dkim; bh=Xs6hjsnOsLry/yDSCPIoYzsRK+ddfUi+o99n3sD7LgI=; b=S8EHFNpthh+A8phZuuQX1UTGyRK0koYo+gqDt2gQC329sn2tMURGXiQUxSPbCvB7m3lgsUB4LuOp/olZbz0IbUeVamQxkk6dKXGJbir8yhA0349jLzmLyNaATX2DsLsGukpoLtEArRPDYJ0r0kiJXWHiGXv1oAt22ziFZMy57I724cQQw5RcaOct2HpFyfGNOCiW0AD+i+64UHxMThj25LKrDbQsbocjhPweWlpwkF7nCPD0kA36bNCyPCi8zmE0v9W3k+njA0vPs0j+p0ITxTyIY7cfSj9G7GU0R6jpsgLN4HjnPtkSt398FTHThXpNg/J58pEE7gQkOBUKkEhzQ==

This signature includes multiple components, including: the DKIM version, the algorithm for canonicalization for message body and headers prior to generating the hash and signature, the selector referenced in the DNS entry, and the base64 hashes for the message body and for the full message. The body hash applies only to the message body and can be validated without reference to the public key. If the body hash is valid, the receiving mail system will perform a DNS request to access the public key for validation of the digital signature of the message. If all these steps are successful, the DKIM signature is considered valid. Implementation of DKIM is a bit complex, but gives strong confidence to the integrity of the message.

Domain-based Message Authentication, Reporting, and Conformance

DMARC builds on SPF and DKIM, adding an additional layer that enables reporting and accountability in the email ecosystem. Also implemented as a TXT entry in the DNS, DMARC aligns to existing SPF and DKIM entries and provides addresses to send and receive email performance and exception reports. These reports enable a mail administrator to know if unauthorized or invalid messages were sent on behalf of their domain.

Multiple Interrelated Protocols Increase Trust

The implementation of this full suite of email protocols can be a bit complex, even for experienced systems administrators. Fortunately, most libraries will not need to implement them directly. In most cases the vendor of the ILS, event management system, or automated marketing solution will attend to these details. Libraries should, however, require that these vendors demonstrate that these protocols have been implemented and produce fully validated messages. This is especially important if the messages are sent using the library's own domain, which is the preferred approach. Libraries would generally prefer that the messages send on their behalf come from an email address like circulation@mylibrary.org rather than something like circ.mylibrary@vendor.com.

These protocols and procedures provide a basic technical foundation for a library's email messaging environment. With this foundation in place, email can better serve as a component of an overall messaging strategy that includes other channels such as mobile messaging and social media. Many libraries are working toward communications strategies that go beyond support of transactional interactions, such as circulation notices, to also encompass broader campaigns in support of stronger engagement with existing patrons and to reach more broadly into their service community.

Notes

1. Timothy Inklebarger, "Librarians Recruited as COVID-19 Hunters." *American Libraries*. https://americanlibrariesmagazine.org/blogs/the-scoop/contact-tracing-librarians-recruited-as-covid-19-hunters.
2. "Library Re-Opening Strategies Around the World: An Overview of Current Proposals (6 June 2020)," International Federation of Library Associations and Institutions (IFLA), https://www.ifla.org/files/assets/hq/topics/libraries-development/documents/overview_of_re-opening_plans_6_june.pdf
3. "Test Plan for the Natural Attenuation of SARS-CoV-2 as a Decontamination Approach" Battelle, prepared for OCLC and Institute for Museum and Library Services (IMLS), 2020, https://www.webjunction.org/content/dam/WebJunction/Documents/webJunction/realm/test-plan.pdf.
4. REALM Project, https://www.webjunction.org/explore-topics/COVID-19-research-project.html.
5. "Number of sent and received e-mails per day worldwide from 2017 to 2023" Statistica, 2019, https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide.
6. "Global spam volume as percentage of total e-mail traffic from January 2014 to December 2019, by month." Statistica, 2020, https://www.statista.com/statistics/420391/spam-email-traffic-share.

Questions or suggestions for topics in future issues?

Contact Patrick Hogan at **phogan@ala.org**

ALA TechSource
alatechsource.org

Smart Libraries Newsletter
American Library Association
225 N. Michigan Ave., Suite 1300
Chicago, IL 60601-7616 USA
Address Service Requested

NON PROFIT
US POSTAGE
PAID
PERMIT 4
HANOVER, PA

July 2020
Smarter Libraries through Technology

Smart Libraries Newsletter

Marshall Breeding's expert coverage of the library automation industry.

Editor
Marshall Breeding
marshall.breeding@librarytechnology.org
Twitter: @mbreeding

Managing Editor
Patrick Hogan
312-280-3240
phogan@ala.org

Digital Access for Subscribers
journals.ala.org/sln

Production and design by the American Library Association Production Services Unit.

Smart Libraries Newsletter is published monthly by ALA TechSource, a publishing imprint of the American Library Association.

alatechsource.org