ALA American Library Association

PRIVACY AND SECURITY FOR LIBRARY SYSTEMS

Marshall Breeding

Library Technology Reports
Expert Guides to Library Systems and Services

MAY/JUNE 2016
Vol. 52 / No. 4
ISSN 0024-2586

Library Technology
REPORTS
Expert Guides to Library Systems and Services

Privacy and Security for Library Systems

Marshall Breeding

ALA TechSource
alatechsource.org

American Library Association

Library Technology
REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 52, Number 4

Privacy and Security for Library Systems

ISBN: 978-0-8389-5972-5

American Library Association

50 East Huron St.
Chicago, IL 60611-2795 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Advertising Representative

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

Editor

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

Copy Editor

Judith Lauber

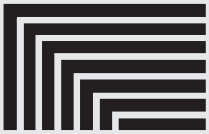
Production

Tim Clifford and Alison Elms

Cover Design

Alejandra Diaz

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 50 E. Huron St., Chicago, IL 60611. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to Library Technology Reports, 50 E. Huron St., Chicago, IL 60611.



About the Author

Marshall Breeding is an independent consultant, speaker, and author. He is the creator and editor of Library Technology Guides (www.librarytechnology.org), editor of *Smart Libraries Newsletter*, and a columnist for *Computers in Libraries*. He has authored the annual "Library Systems Report" feature published most recently in *American Libraries*. He has also edited or authored several books, including *Cloud Computing for Libraries*. Formerly the director for innovative technology and research for the Vanderbilt University Library, he regularly teaches workshops and gives presentations internationally at library conferences. This is his thirteenth issue of *Library Technology Reports*.

Abstract

Having surveyed vendors and ARL libraries, Marshall Breeding covers the current state of patron privacy in interacting with the library's web-based systems. *Library Technology Reports* (vol. 52, no. 4), "Privacy and Security for Library Systems," discusses key technologies and techniques for protecting patron privacy, focusing on encryption, the storage of data, the catalog, and discovery systems. It explores the many ways patron data and behavior may be captured in the absence of preventive measures.

Get Your *Library Technology Reports* Online!

Subscribers to ALA TechSource's *Library Technology Reports* can read digital versions, in PDF and HTML formats, at http://journals.ala.org/ltr. Subscribers also have access to an archive of past issues. After an embargo period of twelve months, *Library Technology Reports* are available open access. The archive goes back to 2001.

Subscriptions

alatechsource.org/subscribe

Contents

Chapter 1

Issues and Technologies Related to Privacy and Security

Libraries have a long tradition of taking extraordinary measures to ensure the privacy of those who use their facilities and access their materials. An important value surrounds the concept that individuals can access or read any material offered by the library without concern that their selections will be made available to any other person or organization. There are many scenarios involving sensitive topics where exposure of items accessed in the library or borrowed can be not just a point of controversy or embarrassment, but also a matter of personal danger.

The American Library Association addresses privacy in one of its interpretations expanding on the Library Bill of Rights, leading with this statement:

> Privacy is essential to the exercise of free speech, free thought, and free association. The courts have established a First Amendment right to receive information in a publicly funded library. Further, the courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy.[1]

The policies, processes, and procedures that libraries embrace related to print materials have been well established. Libraries regularly operate the automation systems that manage the circulation of physical materials in a manner that minimizes any possible exposure of personally identifiable information related to a patron's check-out activity. During the period of an active loan, the automation system maintains a link between the specific patron record and the item borrowed. This information, which is needed to manage the loan transaction, through linking content with an individual, would by privacy policies be treated with strict confidentiality by any library personnel with operational or technical access. Circulation systems need to be able to link content to an individual in order to ensure the return of materials and enable the sending of messages regarding items overdue, fines, or recalls. Past the point of operational need, many libraries will take measures not only to disassociate the item from the patron, but also to anonymize the transaction in a way that the link cannot be reconstructed. Such anonymization would support any historical or statistical reporting the library may need, but ensure that it is not possible to reconstruct borrowing history for any patron. These procedures protect this sensitive information from accidental exposure or from access by unauthorized individuals, as well as from requests from law enforcement or other authorities.

This issue of *Library Technology Reports* focuses on patron privacy related to how patrons interact with a library's web-based systems to access information. Since most libraries offer considerable content and services through the web, the extent to which a patron's use of these services might be vulnerable to exposure stands out as a topic of critical interest. The second statement of the ALA interpretation on privacy is especially relevant to the discussion:

> In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf. Confidentiality extends to "information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA Code of Ethics), including, but not limited to:

> database search records, reference questions and interviews, circulation records, interlibrary loan records, information about materials downloaded or placed on "hold" or "reserve," and other personally identifiable information about uses of library materials, programs, facilities, or services.[2]

One of the specific concerns surrounds how well the privacy of a patron is protected when accessing a resource provided by the library via the web. That patron may be accessing that resource from equipment inside the library itself, from a home or office computer, from the wireless network in a coffee shop, or from a distant and sensitive geographic location.

A patron's session accessing a library-provided resource can be seen as similar to a circulation record and must therefore receive the same kinds of measures to ensure its privacy. Such a session may include the sequence of data that describes a query entered into a search box, lists of items returned by the service, and items selected, as well as the text of any materials read online or downloaded. Even when a resource is accessed without an explicit sign-in, many technical clues may be available that link that session to a specific location or individual. If captured by any third party, such a bundle of information would expose even more private data than a circulation transaction.

The January 2015 issue of *Smart Libraries Newsletter* addressed library privacy and security, including a preliminary version of the vendor survey included in this report. The introduction to that study likewise provides some context to this report:

> In the consumer arena, concern for privacy may not be of central concern. Quite the contrary, details regarding any pattern of behavior that might have a direct or indirect commercial impact have become one of the major currencies of the economy of the Web. Advertising dominates as the primary business model. Very sophisticated networks have been created that gather data from both in-person interactions and online activity, primary for the purpose of targeting advertising content. In person, individuals enable tracking of their purchases through loyalty cards and retailers use many other direct or indirect mechanisms to track buying patterns. Much of the infrastructure of the internet has been infiltrated with technical mechanisms that gather and transmit information regarding the sites visited, terms searched, items purchased. From browser-based cookies to much more sophisticated techniques for tracking online behavior, considerable activity transpires behind the scenes to gather any miniscule item of data that might have some commercial value.
>
> This infrastructure that churns personal activity into targeting advertising provides the fundamental economic model for most services provided via the Web. Much of the entertainment content and productivity tools we enjoy is made possible in return for being exposed to advertisements rather than through direct payment. Facebook, for example, as the dominant social network, thrives on this ad-based economy. Since most individuals would rather not pay directly for each service they use, advertising is tolerated on the current online media just as it has been for television throughout its history.
>
> Given the pervasive gathering and transmission of personally identifiable information on the Web surrounding ad-based commerce, libraries have to be very aware of its impact on the services they deliver.
>
> As libraries offer services that allow their community members to search their collections of print, electronic, and digital resources and to access an increasing body of content online, it is critical to maintain privacy if the same ethic that has been historically held for print resources is applied to their online offerings. Given the pervasiveness of advertising networks in the deep infrastructure of the Web, libraries have to work quite hard to even know how much personally identifiable information is transmitted from the services they deliver to third parties. As libraries work to enrich their online presence with a social flavor, they may inadvertently also enable an intermingling of commercial infrastructure into the services they provide.
>
> One of the realities of the Internet lies in the ability for any third party to intercept the transmissions of information as it travels among devices and servers. Wireless networks are an especially easy target. It has to be assumed today that any information transmitted as clear text across a local network or the Internet will be intercepted and used. These purposes range from gathering personal data that might be of use for targeted advertising, to capturing data that might allow the intrusion into servers and systems to gain access to passwords, credit card numbers, sensitive documents, or other items of value.[3]

This issue of *Library Technology Reports* discusses some of the key technologies and techniques related to protecting the privacy of patrons as they interact with web-based services provided by their library. It focuses on encryption as the primary technology for protecting the privacy of online behavior, how data is stored internally, and other features that may be offered in online catalog and discovery products. This report includes two related studies. One is based on a questionnaire sent to providers to assess the capacity of the major discovery interfaces in resource management systems related to patron privacy and security. The other study examines the websites, catalogs, or discovery interfaces of large academic and public libraries, noting characteristics such as the use of secure communications and the presence of commercial tracking agents.

This report does not aim to prescribe or advocate for any specific set of privacy policies. Rather,

it focuses on the technology issues surrounding privacy for those interested in not exposing personal information or search behaviors of their patrons who use library-provided web-based services. This report explores the many ways in which patron data and behavior can be easily captured in the absence of preventive measures.

Privacy for Circulation Records as a Model

Libraries treat records related to physical circulation according to practices that reflect their policies for privacy and security. These policies may include minimizing any links between content items and patron records. From an operational perspective, it is necessary to record a link between a patron record and an item that has been loaned to a patron. This link underlies the ability to track when items are due, to send reminders and notices, and to enable the patron to view lists of items currently charged and to perform renewals and other self-service actions. Once the item has been returned, many libraries will activate features of their integrated library system to disassociate the link. Data regarding a specific item borrowed by a specific patron is often anonymized, preserving only categories of items or patrons for statistical purposes. Some systems will retain a patron record identifier in an item record after it has been returned for a limited time in order to be able to trace problems. This data may then be erased or overwritten once the item is loaned to a patron.

To ensure privacy, the anonymization of library circulation transactions may be applied both to the operational databases and to any log files that reflect the transactions. Integrated library systems, like other business applications, create log or journal files that record the details of all transactions performed. These log files both provide a historic record of activity to generate statistics and also can be part of a disaster prevention and recovery procedure. In the event of a system failure, any transactions not included in backups used to restore the database can be replayed from the log files. This is a possible strategy to restore transactions that took place between the last backup and the time of the failure. A thorough anonymization of personal information must also include these transaction log files, since they could be used to reconstruct the links between content items and specific patrons.

Active database files and transaction logs will usually be backed up through routine disaster recovery procedures. Libraries interested in completely anonymizing circulation records will need to address what personal data may be retained in backup replicates. A thorough set of disaster avoidance and recovery procedures provides many layers of protection against data loss, which also makes it challenging to ensure that none of the backup copies can be used to reconstruct personalized information.

The procedures related to patron privacy are generally intended to protect specific data regarding patron reading behaviors. Destroying or anonymizing circulation records ensures that private information cannot be accidently or intentionally exposed to unauthorized parties. These procedures also protect the user of a library in cases where law enforcement authorities make a request. With thorough technical procedures in place designed to protect privacy, no personal data would exist that might be subject to such requests.

Privacy and Security for Web-Based Services

The level of attention given to circulation records to align with privacy policies may also be applicable to library websites and discovery services. The operational and technical complications involved in maintaining the privacy of circulation systems demonstrate the complex operational and technical measures involved. Similar concerns apply to patron activity conducted to access the library's web-based resources and services. Transmission of patron sessions over the Internet evokes similar issues and requires proactive measures to maintain consistency with library privacy policies. To protect privacy, organizations need to consider the protection of both "data in motion" as it traverses networks and "data at rest" as it is stored on servers. This report considers both scenarios.

The technology infrastructure of the web poses many challenges to libraries that aim to preserve patron privacy and maintain high security. Any information transmitted via the Internet, as a public network, can be easily accessed by any third party unless specific measures are taken. Web servers and associated software may expose data that may not be consistent with privacy policies. It is important for libraries to understand what information is transmitted and stored by their web-based systems in order to be able to operate these systems in ways consistent with the applicable policies.

The protocols used in the transmission of data on the Internet make it relatively easy for anyone to intercept and view that content and therefore have a direct bearing on privacy and security. The tools to eavesdrop on Internet traffic are easily acquired and do not necessarily require specialized expertise to operate. Any content transmitted over the Internet must be considered publicly viewable unless specific measures, especially encryption, are taken to protect it. But with encryption in place, such interception of data becomes almost impossible.

Basics of Secure Transmission Technologies

No network can be considered safe for the transmission of "clear text," or unencrypted data. There are just too many possible points of interception. Wireless networks provide the most convenient opportunity for gathering information via eavesdropping techniques. Any person equipped with a mobile device and easily obtained software can view all the unprotected data passing through that wireless access point. Wired networks can also be vulnerable to anyone able to physically connect. Other points of vulnerability include the organizations that provide network services. Internet service providers are able, and may be required, to capture Internet traffic and provide access to third parties, such as governmental entities.

Encryption is the primary technique used to protect data from unwanted access by third parties. It protects data transmitted across networks and stored on computers. Encryption algorithms transform data before it is transmitted into a seemingly garbled form that, if intercepted, cannot be deciphered. Most encryption technologies in use today rely on a scheme called public key infrastructure (PKI). Data is encrypted with a private key and digital signature feed into a software algorithm. The data can be decrypted with the corresponding private key. Secure communication on the web provides two important benefits: it authoritatively identifies the website, and it enables encrypted communications between the user's browser and the server providing the resource.

Without entering the deeply technical realm of encryption, there are some high-level concepts relevant to a discussion of library privacy and security concerns. The PKI infrastructure in use on the web provides secure communications by both validating the identity of a site and by transmitting data using encryption. The identity of a website transmitting securely is validated through a digital certificate. Certificates are issued through organizations that confirm the identity of the entity and are based on a hierarchy of trust. Since much of the web, especially those sites involved in e-commerce, depends on secure communications, the digital certificates used by web servers are carefully controlled. It is also possible to use self-signed certificates internally within an organization, but their use for external transactions would be apparent and flagged as not trusted. Credentials of organizations are validated before a certificate is issued by a reputable certificate authority. Compromised or otherwise problematic certificates can also be revoked. Standard validation procedures include checking certificates against revocation lists.

Digital certificates can be installed into a web server to enable encrypted transmission. When activated, pages will be transmitted using the HTTPS protocol rather than HTTP. In most cases, HTTPS traffic is associated with the TCP/IP port 443 and HTTP with port 80, although other port assignments are common. The user's browser will show an indication that the transmission is secure. Chrome, for example, presents a fully valid secure site with a green padlock and shows HTTPS in the URL, and clicking on the padlock will display the details of the certificate. Relevant details include the identity of the organization to which the certificate was issued, the certificate authority, and the technical protocols used for transmission and encryption. Before performing a sensitive transaction, a user can verify that the digital certificate indeed matches the intended organization.

Modern encryption technologies protect data even when massively powerful computers attempt to break them by brute force, such as rapidly trying all possible combinations that constitute a password or key. As computers become ever more powerful, the strength of those algorithms must likewise be improved through techniques such as longer keys. Out-of-date encryption technologies must therefore be considered insecure. A modern web browser will usually detect such vulnerabilities.

Web browsers will display the indicators of a secure transmission only when specific technical criteria have been met. Criteria include the presence of a valid certificate (including checking revocation lists) as well as current technologies for transmission and encryption. Encryption must be performed with a key of sufficient length and according to an algorithm able to defy decryption attempts. This age of massively powerful computation resources capable of decryption attempts by brute force demands the utmost caution in implementing security. The SHA-1 algorithm, which had been widely used for encryption, is now considered vulnerable, replaced by more robust protocols such as SHA-256. The secure sockets layer (SSL), in addition, is now considered obsolete and untrustworthy, with TLS 1.2 currently accepted as the trusted protocol for secure transmission on the web. Since 2014, Chrome and other browsers will flag as untrusted web servers that continue to use SSL. In 2016, it is also anticipated that sites relying on SHA-1 will likewise be flagged as untrusted. The technologies used to support communications should be considered a constantly moving target. Website operators and users who rely on secure communications must be ever vigilant and stay abreast of current standards.

The use of secure communications provides the best approach possible today for protecting the privacy of patrons as they interact with library systems. A page remains encrypted from the time it is transmitted by the web server until it is displayed on the user's browser. As a result, the information remains impervious to eavesdropping through the complete route, even if it includes unsecured wireless networks or

other points of vulnerability along the way. Likewise, any information passed in the clear without encryption should be assumed to be publicly viewable.

Secure Storage

The details on secure communications apply to pages as they are transmitted from servers on the web, the concern for "data in motion." Another set of concerns relates to how data is stored. Data can be encrypted when it is stored on a network server or storage device. Such encryption would protect the data in the event of successful penetration into a server by an unauthorized entity. The most common scenario involves passwords, for which standard practice requires that they be stored in an encrypted hash and never as clear text. When a password is stored as a hash, even the site operator cannot view it. An authentication request can compare the hash of the string provided against that of the password when it was created, but the password itself cannot be reconstructed. Other sensitive elements, such as credit card numbers, would also be stored in encrypted form. Some applications designed to operate with a high level of security may also encrypt other details. For most library-related applications, routine transaction data and logs are not encrypted and depend on general system security to prevent unwanted access.

Locally Managed or Remotely Hosted

Integrated library systems, discovery services, and other library-related software may be deployed either as software that the library installs within its own technical infrastructure or as a service hosted by the vendor. The same kinds of concerns apply in either scenario. For a locally installed system, the library would bear more responsibility for its secure operation and for the procedures implemented to guard privacy and security. Hosted systems naturally place more of that burden on the vendor. Even when a system is hosted by the vendor, the library will want to understand and hopefully control the procedures in place.

The deployment methods used in hosted systems also come into play relative to these issues. One deployment model involves the hosting of individual physical or virtual servers. The same configuration options and operational procedures apply whether these server-based systems are hosted by the library or by the vendor. Each library's instance of the software can be configured individually. One library might, for example, instruct the vendor to configure the server to encrypt all traffic related to its online catalog while other libraries opt to operate without that capability. The options and features available may also depend on the version of the software implemented, which may differ across the libraries using that system. Multi-tenant platforms, where all the libraries using that system share the same instance, have the capability for uniform security configuration. It is possible for the provider of a multi-tenant application to enforce encryption for all its customers using the software. The Apollo ILS and the BiblioCore discovery service both, for example, enforce secure communications for all transactions.

Whether the servers that host the library's integrated library system, discovery service, or other systems are installed locally in the library or by an external provider impacts the route through which a patron's session is transmitted. In most cases the physical location of the service relative to the user is neutral relative to privacy concerns. Even if the user and the server were on the same local area network, the possibility remains that the transmission could be captured by others on that network or beyond. Library systems hosted externally, or content services provided over the web from the publisher's servers, traverse many intervening networks and exchange points and must be considered as vulnerable. Whether remote or local, patron sessions should be managed with encrypted transmission to ensure privacy.

In addition to the ability to capture data describing a patron session via network transmission, there are other points of vulnerability for patron privacy in a routine web session. The techniques used to support use statistics, analytics, and interactions with other services may result in exposure to external entities.

Server Logs Record Patron Activity

It is essential for any organization operating a website to be able to measure and monitor its use. In the same way that libraries often count the number of visitors to their physical facilities, the number of items loaned, reference questions received, and other services, they also track how their virtual services are accessed via their website. Use data for web-based services not only helps demonstrate the impact of the library to funding agencies and administrative authorities, it also provides essential information for designing and tuning the site to function optimally. Both commercial and nonprofit organizations that rely on their websites for critical aspects of their operations benefit from gathering extensive data regarding use patterns and performing analysis to be able to identify problems or to optimize navigation or presentation or to make other changes to improve usability and eliminate problems. The use of web analytics has become part of the essential tool kit for website administrators and user experience specialists.

Web analytics depends on data describing each interaction that takes place on the site. Web servers can be configured—and usually are—to record every page request in a log file. It is important for these server logs to be a component of the technology covered by privacy procedures. For any web server that delivers access to library services and content, these logs capture and retain details of patron interactions that may be sensitive. Server logs almost always capture every request issued, tied to a specific IP address. That IP address in itself may or may not be able to be traced to a specific individual, but it may provide clues to physical location, and data from other sources may be able to link that IP address to some level of identification.

Reviewing a few of the basics of what happens when viewing a website helps underscore the privacy concerns. In response to a request, usually evoked by clicking on a link or pressing a form button, the web server transmits a file corresponding to the URL, encoded in some flavor of HTML or XML, to the IP address associated with the web browser making the request. The entire transmission, including the URL, the page requested, any embedded scripts, and data associated with a POST directive, can, if it is not encrypted, be captured through eavesdropping hardware or software and viewed.

The web server will also record the request in its log. What the server records in its logs depends on how it was configured, but a typical log entry might resemble this one from Library Technology Guides, with the following selection of fields:

```
2016-01-03 22:56:13 64.150.189.27 GET
/libraries/search.pl ILS=Alma 80 -
107.133.80.235 Mozilla/5.0+(Windows+
NT+10.0;+WOW64)+AppleWebKit/537.36+(
KHTML,+like+Gecko)+Chrome/47.0.2526.
106+Safari/537.36 200 0 0 780 http://
librarytechnology.org
```

Which can be presented in a more readable way:

- **Date and Time Stamp:** 2016-01-01 22:56:13
- **Server IP:** 64.150.189.27
- **Method:** GET
- **URI Stem:** /libraries/search.pl
- **Query String:** ILS=Alma
- **Port:** 80
- **Client IP:** 107.133.80.235
- **User Agent:** Mozilla/5.0+(Windows+NT+10.0;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/47.0.2526.106+Safari/537.36
- **Response Code:** 200
- **Bytes Transferred:** 780
- **Referrer:** http://librarytechnology.org

Server logs preserve a great deal of information describing a visitor session. In addition to the exact time the resource was requested, other information includes the previous page or site that the browser requested. This "referrer" data provides interesting information about what other resources funnel users to the site and internal navigation.

It should also be noted that the query string can reveal specific information about search behavior. In this case, it shows that the request involved a search for libraries using the Alma ILS. In this case, the query string was presented as part of the URL in a GET directive. If the POST directive were used instead, the same information would be transmitted via a separate data stream and placed on a temporary file on the server.

Subsequent entries from the same session would show what specific entries from the search results were displayed. This data describing information-seeking behavior is transmitted across the Internet and stored in server logs.

As we will explore in more depth below, these same mechanisms apply to online catalog, discovery service, or other library interfaces, where the behavior involved may include a search issued by a library patron, lists of items held by the library, and which specific title was selected. In the case of an e-book or other electronic resource, this data at least implies reading behavior. These sequences of data represent patron interactions that fall into the same level of concern as circulation records for physical books. These categories of data may or may not be covered by any given library's privacy policies, but it is important to understand the technical reality that search and reading behavior is routinely exposed in the operation of web-based resources.

The data transmitted by the example above does not necessarily include personally identifying information. But it does include contextual data with the potential to be narrowed to a specific individual. The IP address identifies the device associated with the request. In some cases, the computer routinely used by an individual may have a fixed IP address, which then represents a strong link to a specific person. In other cases, the IP address recorded may be the router to the network connecting a household, organization, or larger set of devices to the Internet. The common practice of dynamically issued IP addresses further weakens the link between an IP address and a given individual.

The application generating the page transmitted may operate with additional levels of personal data. Any site with the ability for users to register and sign in with a personal account will have the potential to associate that account to specific online behaviors. In some cases, that profile can be associated with a username or handle not necessarily validated to an individual in real life. In other cases, that profile may

be linked and validated to a specific individual. The automation systems used by libraries, for example, are usually validated to a specific individual with personal details such as physical addresses, phone numbers, and demographic details.

In previous times, library accounts would frequently record Social Security numbers or other official identification numbers. Fortunately this practice has largely been abandoned. Academic libraries, for example, would instead record the identification number issued by the educational institution.

From a privacy perspective, the application must securely contain personal details and behavior internally and not allow these details to be exposed externally, according to the policies and procedures in place relating to the confidentiality of patron records. Queries performed, titles selected, items currently and previously checked out, or lists of favorite items are some of the elements that may be internally stored in association with a patron's record or profile within an integrated library system or discovery environment, expanding the scope of concern beyond the records stored in databases to the log files of any web servers involved.

Tracking Tags and Web Beacons

Another mechanism that has become a routine part of web-based systems involves the use of what are commonly called web beacons or tracking tags. These tags are bundles of information sent to an external service to perform a specific function. Tracking tags may support analytics related to website usage, performance monitoring, or management of advertising content.

One of the most popular—almost ubiquitous—uses of tracking tags can be seen in sites configured for Google Analytics. This service, which Google makes available without cost, operates on the basis of collecting data transmitted with each page request. Website managers enable Google Analytics by establishing an account that is assigned an organizational identifier. Using the Google Analytics administrative tool, a snippet of code is produced that includes an institutional and site identifier, which is embedded on each page. This snippet executes JavaScript that is programmed to send specific data to Google's servers with each page request.

Google describes the categories of information it collects for any of its services.[4] The Google Analytics Developers pages provide more specific information transmitted to Google's servers for any page request.[5] At least the same level of data is sent to Google as is captured on local web server logs. But in addition to the user's HTTP request and the signatures of the web browser and the operating system of the user's computer, Google also captures contents from cookies. The first-party cookies authorized to be accessed include any from the Google family of products, which also includes the AdSense and DoubleClick advertising services.

The transmission of these data elements through web beacons to Google or other organizations does not necessarily include personally identifiable content. These data elements include details regarding the page requested, the previous page visited, time stamps, the IP address of the requestor's browser, and cookie data that provides considerable information regarding the session. It's also possible that non–personally identifiable information from a library search session might be linked with personally identifiable content captured from that individual's access to other non-library sites, with inferences of identification. If a visitor to a site that uses Google Analytics is signed into his or her Google account, there may be an increased possibility that activity carried out on that page could be directly linked to that account holder.

Mayer and Mitchell describe the privacy issues involved when a web page enables a tracking code to a third-party site:

> Web browsing history is inextricably linked to personal information. The pages a user visits can reveal her location, interests, purchases, employment status, sexual orientation, financial challenges, medical conditions, and more. Examining individual page loads is often adequate to draw many conclusions about a user; analyzing patterns of activity allows yet more inferences.
>
> When a first-party page embeds third-party content, the third-party website is ordinarily made aware of the URL of the first-party page through an HTTP referrer or equivalent. If the page embeds a script tag from a third party, the third party will also often learn the web page's title from `document.title`. Some first parties will voluntarily transmit even more information.[6]

The insertion of web beacons into library-branded pages at a minimum expands the matrix of organizations with technical data describing any given element of online behavior. The data may or may not cross any thresholds of privacy. It does seem important for libraries to be fully aware of the data transmitted to any third party relative to actions performed by their patrons through resources they provide. This report includes a survey of library websites that itemizes the web beacons detected. No further analysis was conducted to discern the specific information transmitted. This survey was conducted primarily to observe the degree to which libraries include these web beacons and which organizations receive any data regarding patron transactions carried out on library sites.

Libraries may want to conduct a thorough audit of their websites and services to gain a detailed understanding of what information is transmitted to any

third parties through web beacons or similar techniques. Including these devices can be defended from a privacy perspective based on confidence of what data is transmitted and trust in the organization receiving that data. In some cases, web beacons may be enabled casually or even accidentally. It is common to include scripts and code from other sources without an exact understanding of what beacons may be embedded or what code may be executed on third-party sites.

The following two chapters include two empirical studies that relate to the treatment of privacy on library websites and discovery services. Chapter 2 provides data from a questionnaire completed by a selected set of vendors offering online catalog or discovery services that probes their capabilities and strategies regarding encryption of data transmitted and stored within their systems that may include personal information. Chapter 3 reflects data collected from two sets of large libraries regarding the secure transmission of library websites, catalogs, and discovery services and the presence of web beacons detected on the sites.

The use of cookies, another technique with privacy implications used by websites, is not covered in this report. Cookies are small data files that a web page may deposit on the computer used for session continuity, personalization features, and management of advertising content. In most cases, a cookie can be accessed only by pages associated with the organization that created it. This organization may span multiple entities with different services and activities. Google, for example, may share cookie content among its properties, including AdSense and DoubleClick. Opportunities for further study would include the use of cookies by library websites and catalogs.

Notes

1. "An Interpretation of the Library Bill of Rights, Privacy," American Library Association, accessed January 10, 2016, www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.
2. Ibid.
3. Marshall Breeding, "Smarter Libraries through Technology: Protecting the Privacy of Library Patrons," *Smart Libraries Newsletter* 35, no. 1 (January 2015): 1.
4. "Information We Collect," Privacy, Google, accessed February 8, 2016, www.google.com/policies/privacy/#infocollect.
5. "Tracking Code Overview," Google Analytics, accessed February 8, 2016, https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview?csw=1.
6. Jonathan R. Mayer and John C. Mitchell, "Third-Party Web Tracking: Policy and Technology," in *Proceedings: 2012 IEEE Symposium on Security and Privacy, S&P 2012* (Los Alamitos, CA: IEEE Computer Society, 2012), 3, http://dx.doi.org/10.1109/SP.2012.47, available online at https://jonathanmayer.org/papers_data/trackingsurvey12.pdf.

Chapter 2

The Current State of Privacy and Security of Automation and Discovery Products

This chapter presents the results of a survey presented to vendors to gather information regarding the general characteristics of some of the major integrated library systems, library services platforms, and discovery services related to how well they defend patron privacy and handle overall security.

A questionnaire on this topic was developed and sent to Auto-Graphics, Biblionix, BiblioCommons, Ex Libris, Innovative Interfaces, OCLC, and Sirsi-Dynix and to the development communities for Koha and Evergreen. These organizations were selected to represent a mix of systems that find wide use in the United States. This report is not intended to be a comprehensive study but to provide a look at the current state of privacy and security options based on some of the major providers. This study covers the following companies and products:

- **Auto-Graphics** develops and supports the VERSO ILS used primarily by public libraries.
- **BiblioCommons** offers a variety of patron-facing products through a large-scale web-based platform that interoperates with most of the major ILS products.
- **Biblionix** offers Apollo, a purely web-based ILS for small public libraries delivered through a multi-tenant platform.
- **EBSCO** offers EBSCO Discovery Service, which ranks as the most widely used index-based discovery service. This product can be used as the catalog interface for any integrated library system in addition to providing article-level search for a library's collection of electronic resources. The product includes an API so that its results can be integrated into other catalog or discovery environments.
- **Innovative** now supports an expanded slate of library management products including Millennium Sierra, Polaris, Virtua, and Sierra as well as discovery services such as Encore and Chamo.
- **SirsiDynix** products include Symphony and Horizon as its major ILS offerings as well as the web-based BLUEcloud suite. Portfolio is the company's faceted discovery interface; eLibrary is the online catalog module associated with Symphony; iPac is the online catalog module for Horizon.
- **OCLC** has developed its WorldShare Management Services and the WorldCat Discovery Service as global multi-tenant platforms used by libraries of all types. OCLC's earlier discovery interface, WorldCat Local, continues to be used, though it will eventually be replaced by WorldCat Discovery Service.
- **Ex Libris**, oriented primarily to academic and research libraries, has developed Alma and Primo as its current set of strategic products for resource management and discovery. The company's legacy ILS products Aleph and Voyager continue to be used in many libraries along with their web-based online catalog modules.

Two open-source integrated library systems are established as major products. As these products are open-source software, libraries implementing them can configure and customize them in a variety of ways, making it more difficult to provide definitive responses to the questions in the survey. The responses that are reproduced here were given by members of the development community for both products for the 2014 issue of *Smart Libraries Newsletter*. No updated response was provided for the 2015 questionnaire, though there are no significant applicable changes.

- **Koha** is an open-source ILS developed by a global community of developers and is used by thousands of libraries of all types around the world.
- **Evergreen** is an open-source ILS, with Equinox Software serving as the dominant development and support firm, supplemented by a global community of developers; it is used primarily by consortia of mostly public libraries in the United States and Canada.

Online Catalog or Discovery Patron Interactions

The initial set of questions focused on how the various products handled transactions conducted by library patrons. Key areas of concern include how well the authentication credentials of patrons are protected and whether all or parts of the session that the patron conducts on the system are protected from detection by a third party as they pass through local networks and the Internet.

Encryption of General Patron Activity

The gold standard for products used by patrons would be to encrypt all traffic conducted by patrons. This level of security would provide very private communications for the patron, with very little possibility for leakage and meaningful detection of content by any third party. In the absence of the encryption of the full patron session, third parties can fairly easily intercept data that reveals the search terms entered by a patron and referral data that shows previous sites visited, results presented, and items selected or downloaded for viewing. Full enforcement of encryption requires that the library or its vendor obtain valid digital certificates, perform needed server configurations, and provide the additional processing resources required. Traditionally, library systems have used encryption selectively. Some providers may not enforce encryption by default, but may enable libraries to select encryption for specific transaction types as an option. The questions in this section walk through these possibilities.

Privacy and Security Questionnaire for Providers of Library Discovery or Resource Management Services

The following instructions were provided to vendors responding to the questionnaire:

> This questionnaire requests information regarding the technical mechanisms in place in your discovery interface or resource management system related to the protection of patron privacy and general security concerns. This questionnaire is similar to the one that was previously submitted for the January 2015 issue of *Smart Libraries Newsletter*. The results of this update survey will be used in an issue of *Library Technology Reports* to be published by ALA TechSource in early 2016.
>
> I would greatly appreciate it if you could have your technical or product managers provide responses to these specific questions. It would also be helpful to have any additional comments or perspective whether these seem to be the best areas of concern regarding patron privacy, if there are alternative strategies that you are pursuing. I would also be interested to hear whether this topic has been raised also by your customers or users through enhancement requests or other product roadmap priorities.
>
> **Background**: The session during which a patron searches a library interface can include sensitive information that should be protected from interception or delivery to any third party. In the same way that library ethics prevent the disclosure of physical items checked out, any information regarding the patron's online interactions should also be protected. A search session can convey items of interest entered by the patron into a query box, lists of items returned as results to that query, items selected, and any items read online or downloaded. In an unencrypted session, all these items describing reading behavior can be intercepted on [a] wired or wireless network unless its transmission is encrypted between the browser and the server operated by or on behalf of the library.
>
> In addition to the search, selection, and reading behavior, patron sessions can also include sign-on transactions, transmission and display of personal details stored in the patron's profile or account, reading lists, check-out history, or other personally identifiable information.

Online Catalogs or Discovery Interfaces

Does Your Online Catalog or Discovery Interface . . .

. . . ENFORCE ENCRYPTION THROUGH HTTPS FOR ALL TRANSACTIONS INVOLVING PATRON ACTIVITY?

Answering yes to this question means that all web traffic transmitted by the application will be encrypted and that there is not an option to disable this feature.

Auto-Graphics

Vendor response: No.

[*Breeding comment:* Encryption of the online catalog for VERSO is an optional feature. The vast majority of libraries using this product have not enabled this feature. Auto-Graphics listed William Hessel

Library of Lake Michigan College as an example of a VERSO site with an encrypted catalog.]

BiblioCommons

Vendor response: Yes.

[*Breeding comment:* All traffic is encrypted in the currently deployed version of BiblioCore. This behavior can be seen in all of the libraries that have implemented BiblioCore as their discovery service. The company shifted to secure transmission of its service in 2015.]

Biblionix

Vendor response: Apollo's online catalog enforces HTTPS for all patron activity. There is no option for patron data to cross the wire unencrypted.

EBSCO

Vendor response: HTTPS encryption is fully supported. Note that users of EBSCO products are not typically known to us as individuals. A link to EBSCO's privacy policy is displayed on its products' interfaces, as well as on its public-facing Web site. It can be reviewed here: http://support.epnet.com/ehost/privacy.html.

[*Breeding comment:* While supported, HTTPS is an optional configuration for EBSCO Discovery Service. When visiting library websites, both encrypted and nonsecure implementations can be observed. The study of ARL libraries below (in chapter 3) includes examples of both configuration options.]

Ex Libris

Vendor response: Ex Libris uses AES encryption standards to keep data in transit encrypted. Alma and Primo support HTTPS enforcement of all communication including staff and patron to encrypt transactions. Alma enforces encryption through HTTPS for all transactions. Primo enforces encryption through HTTPS for staff users and for patron login. In addition, libraries can opt to use HTTPS for all other patron activities.

[*Breeding comment:* As Ex Libris states, encryption is an option, but is not currently required for library implementations of Primo. Examples can be seen in the ARL security study of libraries that have implemented secure and nonsecure instances of Primo.]

Innovative

Vendor response for this entire section: Speaking for Polaris, Virtua and Sierra including their respective OPACs, and Encore and Chamo discovery, the answers are essentially identical. Public searching and discovery [in] all systems support and default to plaintext (HTTP) for searching, and automatically enforce SSL (HTTPS) for all pages involving patron details or login credentials. In the interest of completeness, all systems also have the capability of an "all plaintext" (no HTTPS) option which is not used in modern usage, and all systems have the capability for an "all SSL" (all HTTPS) which can be enabled if it is deemed desirable but in practice has not been commonly used. Patrons who wish to use "all SSL" (all HTTPS) can, of course, simply start their search in SSL (HTTPS) with the https:// URI to enforce full encryption on any system. This flow is typical of other search engines and e-commerce implementations, plaintext for searching with user-initiated SSL (HTTPS) supported, and enforced SSL (HTTPS) for patron/customer/financial details.

The details of HTTPS protocol use and arrangements with respect to certificates is also essentially identical for Polaris, Virtua and Sierra including their respective OPACs, and Encore and Chamo discovery. All implementations make use of industry encryption libraries supporting a range of communications protocols and encryption ciphers, and have configuration options to allow, disallow or prefer different protocols and ciphers as security and interoperability demand, for example, to disallow SSL protocol in favor of TLS protocol, or to disallow the use of RC4 stream ciphers. All require the use of a standard commercial digital certificate, and libraries acquire their own certificates from their preferred digital certificate supplier.

OCLC

Vendor response: OCLC's classic WorldCat Local uses a hybrid model where access to personal information is managed through a secure session after logon. In contrast, OCLC's next generation discovery system, WorldCat Discovery, uses HTTPS for all user activities to protect patron privacy.

[OCLC also provided this general statement:]

> OCLC is committed to library privacy and protecting other sensitive information in support of the library community. OCLC has maintained ISO 27001 certification since 2011 and successfully transitioned to the ISO 27001:2013 Standard. Additionally, OCLC completed a Statement on Standards for Attestation Engagements (SSAE) 16 Service Organization Controls (SOC) 1 audit for our WorldShare applications to validate our internal controls over financial reporting and pursuing to demonstrate compliance with the U.S. Federal Information Security Management Act (FISMA) via the U.S. Federal Risk and Authorization Management Program (FedRAMP) as a Compliant Cloud Service Provider (CSP).

[*Breeding comment:* My observations concur with this statement. WorldCat Local conducts search sessions using an unencrypted transmission, selectively encrypting sign-in pages and others that involve personal details. See the University of Tennessee at Chattanooga as an example. WorldCat Discovery Service, introduced recently, can be distinguished by

the *.on.worldcat.org URL and fully encrypts all sessions. See Anderson University Nicholson Library as an example.]

University of Tennessee at Chattanooga
http://utc.worldcat.org

Anderson University Nicholson Library
https://anderson.on.worldcat.org/discovery

SirsiDynix
Vendor response: Yes.

[*Breeding comment:* It appears that encryption is available as an option and is not required for all deployments. The Hawaii State Public Library system can be seen as an example where Enterprise has been configured for nonsecure operation, and the Orange County Public Libraries in California as one that is secure.]

Hawaii State Public Library
http://hawaii.sdp.sirsi.net/client/default

Orange County Public Libraries
https://catalog.ocpl.org/client/en_US/default/

Koha
Out of the box, Koha does not enforce use of SSL. However, every Koha installation can readily be required to use SSL for public catalog and staff interface access.

Evergreen
The Evergreen public catalog requires the use of SSL when logging into the catalog and when accessing all pages that display patron account information or allow the patron to place requests.

. . . OFFER THE LIBRARY AN OPTION TO ENABLE HTTPS FOR ALL TRANSACTIONS INVOLVING PATRON ACTIVITY?

Auto-Graphics
Vendor response: Yes.

[*Breeding comment:* Observation of VERSO sites confirms that enabling HTTPS is an option configurable by a library, with examples of both seen in library sites.]

BiblioCommons
Vendor response: N/A. HTTPS is enforced for all transactions.

[*Breeding comment:* Verified. Not able to find any BiblioCore sites without encryption.]

Biblionix
Vendor response: No response.

[*Breeding comment:* Apollo enforces encryption for all traffic, and libraries do not have the option to enable or disable it.]

EBSCO
Vendor response: Yes. The library administrator may enable HTTPS access at the profile level through the administrative interface.

[*Breeding comment:* The presence of both secure and unsecure EDS sites confirms the availability of this option to libraries.]

Ex Libris
Vendor response: Yes. Please see response directly above.

Innovative
Vendor response: [See general statement provided above.]

OCLC
Vendor response: Because the WorldShare Management Service suite of applications is multi-tenancy, OCLC is unable to selectively enforce HTTPS for individual institutions. However, using WorldCat Discovery ensures that all transactions are protected via HTTPS.

SirsiDynix
Vendor response: Yes.

[*Breeding comment:* There are libraries using both configuration options.]

Koha
At present, standard configurations of Koha would require SSL for either the entire public catalog or none of it; likewise for the staff interface. [Covers multiple questions in this section.]

Evergreen
The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information.

. . . ENFORCE ENCRYPTION FOR SPECIFIC PAGES OR TRANSACTIONS INVOLVING PATRON DETAILS OR LOGIN CREDENTIALS?

This question asked whether sensitive information such as login credentials or patron details are always encrypted regardless of other options offered.

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: N/A. HTTPS is enforced for all transactions.

Biblionix
Vendor response: None.

[*Breeding comment:* Covered by the above response since all pages are encrypted, including those with login or patron details.]

EBSCO
Vendor response: EBSCO employs industry-standard encryption technologies when transferring and receiving consumer data such as patron details or login credentials.

Ex Libris
Vendor response: Yes. Please see response above.

Innovative
Vendor response: Covered in general statement given above.

OCLC
Vendor response: All systems enforce encryption for transactions and logon details.

SirsiDynix
Vendor response: Yes.

Evergreen
The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information.

. . . OFFER THE LIBRARY AN OPTION TO ENABLE HTTPS FOR SPECIFIC PAGES OR TRANSACTIONS INVOLVING PATRON DETAILS OR LOGIN CREDENTIALS?

This question applies to systems that don't automatically encrypt pages that include login credentials or patron details. Libraries can choose whether to send this data in the clear or enable an option to encrypt.

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: N/A. HTTPS is enforced for all transactions.

Biblionix
Vendor response: No response.

[*Breeding comment:* Covered by the above response since all pages are encrypted, including those with login or patron details.]

EBSCO
Vendor response: Yes. EBSCO provides HTTPS as an option for its applications, including transactions involving patron and login details.

Ex Libris
Vendor response: Aligned with industry best practices, we believe that in order to provide high level of security and protect personal data while meeting high security standards, the entire communication of all pages including login, should be encrypted. As such when encryption is used in Primo, the entire communication is being encrypted for all of the pages. With Alma the entire communication is encrypted at all times.

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: All systems enforce encryption for transactions and logon details.

SirsiDynix
Vendor response: Yes.

Evergreen
The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information.

DESCRIBE THE PROTOCOLS USED FOR ENABLING ENCRYPTED TRANSMISSION, SUCH AS TRANSPORT LAYER SECURITY 1.2

Auto-Graphics
Vendor response: Supported protocols: TLS 1.2, TLS 1.1, TLS 1.0; SSL 3 administratively disabled; SSL 2 administratively disabled.

BiblioCommons
Vendor response: Transport Layer Security 1.2.

Biblionix
Vendor response: Biblionix stays abreast of best practices regarding TLS. We use TLS 1.2 for all browsers that support it. TLS versions earlier than TLS 1.0 (that is, SSL 3.0 and below) are totally disabled. Our ciphers are selected for maximum security and privacy: we eliminate weak ciphers, and favor ones which allow connections to have perfect forward secrecy. We prevent downgrade attacks by using TLS_FALLBACK_SCSV. We are working on enabling HSTS (HTTP Strict Transport Security) on the entire biblionix.com domain.

EBSCO
Vendor response: EBSCO offers TLS1.2 2048 bit encryption for data in transit.

Ex Libris
Vendor response: Browser to application server connections are https utilizing TLS 1.0 or 1.2 using SHA 128 or 256 key and AES 128 or 256. The TLS version and key strength are negotiated upon session establishment, between the server and the browser. Encryption channel also covers all Alma and Primo communication including Secured FTP, secured SIP communication and secured communication with email servers.

Innovative
Vendor response: [See general statement provided above.]

OCLC
Vendor response: Secure Socket Layer and Transport Layer Security with a third-party certificate authority.

SirsiDynix
Vendor response: SirsiDynix implements TLS 1.2 for HTTPS in our cloud systems.

WHAT IS THE ARRANGEMENT FOR DIGITAL CERTIFICATES USED FOR ENCRYPTION OF PATRON SESSIONS? IS THE CERTIFICATE PROVIDED BY YOUR ORGANIZATION OR DO LIBRARIES NEED TO ACQUIRE THEIR OWN CERTIFICATES?

Auto-Graphics
Vendor response: Can be acquired either way.

BiblioCommons
Vendor response: Certificate is provided.

Biblionix
Vendor response: Apollo runs securely "out of the box" with our certificate. Libraries have the option of acquiring their own certificate for use with the online catalog. This addresses a security "hole" of hosted ILSes: typically (and unfortunately), patrons see a security certificate that vouches for the vendor instead of the library. Patrons shouldn't have to know who the library's vendor is in order to know they're secure. With this optional (but free) Apollo feature, the online catalog can live at the library's domain with a certificate that belongs to the library, while retaining all the advantages of a hosted system.

EBSCO
Vendor response: EBSCO provides certificates for its applications. No client certificates are needed.

Ex Libris
Vendor response: Ex Libris supplies to its cloud customers digital certificates.

Innovative
Vendor response: [See general statement provided above.]

OCLC
Vendor response: For WorldShare Applications and WorldCat Local and Discovery, OCLC provides certificates from a third-party CA.

SirsiDynix
Vendor response: For cloud systems other than EOS products, SirsiDynix handles the purchasing and implementation of certificates. EOS products have the option for HTTPS to be implemented as an add-on feature. Additionally, should a customer wish to purchase a certificate for one of our cloud-hosted products, SirsiDynix will implement the certificate.

ARE LOGS OR OTHER SYSTEM FILES THAT INCLUDE PATRON SEARCH OR READING BEHAVIORS ENCRYPTED?

Auto-Graphics
Vendor response: No.

BiblioCommons
Vendor response: N/A. Logs are anonymized.

Biblionix
Vendor response: Yes, logs, searches, and circulation data are encrypted as they are stored. And the library can choose to disconnect historical checkouts from patrons after a certain amount of time.

EBSCO
Vendor response: Logs are secured by commercial logging device security controls.

Ex Libris
Vendor response: Logs and other system files do not include personal identifying information.

Innovative
Vendor response: [See general statement provided above.]

OCLC
Vendor response: Log files are not encrypted; however, access is restricted to only authorized personnel and OCLC minimizes the ability to attribute logs from searches to specific patrons.

SirsiDynix
Vendor response: System files are protected by operating system permissions and, as an add-on option, the full file system may also be encrypted. We don't log information that is traceable to an individual. For example, we log searches, but anonymously.

Koha
Such logs are not encrypted.

Resource Management Products

Protection of Personally Identifiable Information in the Staff Interface to a Resource Management System

The following statement was provided to vendors completing the questionnaire:

> Staff access to an integrated library system or library services platform can involve access to personal details about patrons. This information can be intercepted by third parties if transmitted without encryption. Library personnel sessions can also involve access to financial information or other sensitive information about patrons, the library, or its parent institution.
>
> Sensitive data can also be vulnerable if it is stored as clear text. Storing sensitive data with encryption provides additional protection against systematic theft through any security breach.

Questions related to how data are transmitted:

Does Your Client or Interface for Delivering Functionality to Library Personnel . . .

. . . ENFORCE ENCRYPTION THROUGH HTTPS OR OTHER ENCRYPTION MECHANISMS FOR ALL TRANSACTIONS?

A positive response to this question would indicate that all pages transmitted will be encrypted and that there is not an option to disable this security feature.

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO does not offer an LMS or ILS. However, where this is applicable to EBSCO's discovery service, EBSCO provides TLS 1.2 2048 bit encryption for data in transit.

Ex Libris
Vendor response: Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.

Innovative
Vendor response for entire section: Speaking for Virtua, Polaris and Sierra, all systems handle communication uniformly for all pages in the staff facing systems rather than toggling between plaintext and encrypted communications by function or by page. Two systems support SSL for staff client communications, one uses a proprietary non-plaintext communication, not SSL.

OCLC
Vendor response: All sessions for library staff are encrypted via HTTPS.

SirsiDynix
Vendor response: Yes, for cloud systems other than EOS, though HTTPS (TLS 1.2) is also an add-on product for EOS systems. HTTPS is an option for clients which host our products internally.

Koha
The Koha staff interface can be configured to require SSL for all pages, although this is not the default configuration. Most Koha vendors do this as default. [Covers multiple questions in this section.]

Evergreen
The Evergreen staff client uses SSL to encrypt all communications with the Evergreen application server. [Applies to all questions in this section.]

. . . OFFER THE LIBRARY AN OPTION TO ENABLE HTTPS OR OTHER ENCRYPTION MECHANISMS FOR ALL TRANSACTIONS?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO does not offer an LMS or ILS. However, where this is applicable to EBSCO's discovery service, HTTPS is provided as an option for its applications. When enabled, all transactions are encrypted.

Ex Libris
Vendor response: Please see response above. [Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.]

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . ENFORCE ENCRYPTION FOR SPECIFIC PAGES OR TRANSACTIONS INVOLVING PATRON DETAILS?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO does not offer an LMS or ILS. However, where this is applicable to EBSCO's discovery service, EBSCO offers the ability to turn on/off HTTPS as appropriate. Encryption cannot be enabled for specific pages.

Ex Libris
Vendor response: Please see response above.

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . ENFORCE ENCRYPTION FOR SPECIFIC PAGES INVOLVING AUTHENTICATION OF LIBRARY PERSONNEL ACCOUNTS?

Auto-Graphics

Vendor response: [No response.]

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: Encryption cannot be enabled for specific pages.

Ex Libris
Vendor response: Please see response above. [Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.]

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . OFFER THE LIBRARY AN OPTION TO ENABLE HTTPS FOR SPECIFIC PAGES INVOLVING PATRON DETAILS?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO does not offer an LMS or ILS. For EBSCO's discovery service, security measures involving patron details employed by EBSCO are enabled by default.

Ex Libris
Vendor response: Please see response above. [Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.]

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . OFFER THE LIBRARY AN OPTION TO ENABLE HTTPS OR OTHER ENCRYPTION MECHANISMS FOR SPECIFIC PAGES INVOLVING AUTHENTICATION OF LIBRARY PERSONNEL?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO does not offer an LMS or ILS. For EBSCO's discovery service, EBSCO offers the ability to turn on/off HTTPS as appropriate. Encryption cannot be enabled for specific pages.

Ex Libris
Vendor response: Please see response above. [Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.]

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . ENFORCE ENCRYPTION FOR TRANSACTIONS INVOLVING INSTITUTIONAL FINANCIAL DATA (ACQUISITIONS, PATRON FINES, ETC.)?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO provides a discovery service, EBSCO Discovery Service, not an LMS or ILS. Financial data is not transferred or stored.

Ex Libris
Vendor response: Please see response above. [Ex Libris uses industry standards to keep data in transit encrypted. Alma enforces HTTPS encryption for all transactions.]

Innovative
Vendor response: [See general statement above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

. . . OFFER THE LIBRARY AN OPTION TO ENABLE SSL OR OTHER ENCRYPTION MECHANISMS FOR FINANCIAL TRANSACTIONS?

Auto-Graphics
Vendor response: Yes. Encryption is turned on either for the entire product or not at all.

BiblioCommons
Vendor response: Yes—HTTPS is enforced for all transactions.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO provides a discovery service, EBSCO Discovery Service, not an ILS or LMS. Financial data is not transferred or stored.

Ex Libris
Vendor response: As described above the entire Alma communication including the institutional financial system with which the solution integrates, is encrypted

as described above. It is important to note that as part of the Alma integration with financial systems, Alma does not store any or process financial information such as credit card information or perform financial transactions.

Innovative
Vendor response: [See general statement provided above.]

OCLC
Vendor response: See above. [All sessions for library staff are encrypted via HTTPS.]

SirsiDynix
Vendor response: Yes.

Additional Security Measures

Describe any other security measures in place that protect patron privacy as it is transmitted over local networks or the Internet from interception by other service providers or partners. One specific scenario that has been a topic of concern involves the presentation of e-book discovery and lending transactions via library catalogs or discovery interfaces, where external organizations such as Amazon or OverDrive gain access to patron details and reading behaviors.

Auto-Graphics
Vendor response: VERSO uses SFTP to deliver patron data to Unique Management for the library's fine and fee collections. These file transfers are of text data (usually CSV files); they are transmitted over secure FTP.

VERSO uses SFTP to deliver overdue and similar data to Talking Tech's iTiva product for telephone notification. These files are also CSV files and are transmitted securely.

VERSO makes use of the OverDrive APIs in order to facilitate seamless transactions and delivery of eBooks and other e-material from Overdrive. Authentication is managed using OAuth, as required by Overdrive, but the data exchange is not, itself, encrypted.

VERSO makes use of the Recorded BooksAPIs in order to facilitate seamless transactions and delivery of digital media from Zinio and OneClickDigital. Authentication is managed using the Record Books API, but the data exchange is not, itself, encrypted.

BiblioCommons
Vendor response: Patron details and reading behaviours are encrypted whenever they are transmitted over public networks to prevent unauthorized access by external organizations.

Biblionix
Vendor response: Apollo makes no distinction between local networks and the Internet. All traffic is encrypted between the patron's or librarian's browser and our servers.

Our ironclad policy has always been that no patron data should cross a wire unencrypted, and that definitely includes third-party interfaces. The SIP protocol is a particular offender here, since it always exposes sensitive patron data, and doesn't make any accommodation for encryption. We've developed a number of different ways to achieve encrypted SIP, have successfully worked with many vendors on it, and we always refuse to make any unencrypted SIP connection. The traditional ILS vendor will use an IP address filter and call that "security" even as they transmit patron data over the wire in clear text. Our SIP connection method involves client and server keys, so that the identity of each party is cryptographically guaranteed to the other party.

Most other protocols (such as NCIP) are HTTP-based, and our normal HTTPS policy applies to those and provides encryption.

EBSCO
Vendor response: Please review EBSCO's posted Privacy Policy for more information: http://support.epnet.com/ehost/privacy.html.

Ex Libris
Vendor response: Ex Libris implements multi-tiered security audits on different levels, including: security checks and manual code reviews daily, application security vulnerability assessment scans quarterly. The vulnerability assessment scans include use of "Acunetix" tool which lists any potential vulnerabilities in the OWASP Top 10. Ex Libris also conducts at least annually, a security penetration test by an external security company covering the OWASP Top 10 and SANS Top 25 security vulnerabilities as well as other known vulnerabilities. The ISO 27001 certification that Ex Libris passed successfully includes annual external audits to validate that all security measures and mitigations are in place.

Innovative
Vendor response: Speaking for Polaris, Virtua and Sierra, APIs handling patron data support SSL (HTTPS) are password and/or key protected to ensure that information is exchanged securely and only with authorized partners, and authorizations are sufficiently granular to limit information exchanged to the business requirements of the specific partnership, and are not inappropriately broad.

SirsiDynix
Vendor response: Yes.

Koha
Koha can be configured to use an LDAP directory to authenticate staff users and patrons. If configured this way, LDAP-over-SSL can be used to encrypt communications between the Koha and LDAP servers.

Evergreen
Evergreen can be configured to use an LDAP directory to authenticate staff users and patrons. If configured this way, LDAP-over-SSL can be used to encrypt communications between the Evergreen and LDAP servers.

WHAT SECURITY MEASURES DOES YOUR ORGANIZATION REQUIRE RELATED TO THIRD PARTY PROVIDERS OR SERVICES THAT PARTICIPATE IN YOUR DISCOVERY INTERFACE OR ONLINE CATALOG?

Integration with third-party organizations could potentially expose patron details, search, or reading patterns and measures that you have provided to strengthen privacy and security. What security measures does your organization require related to third party providers or services that participate in your discovery interface or online catalog?

BiblioCommons
Vendor response: Many third-party integrations have been implemented on the BiblioCommons service at the request of partner libraries, who have contracted both fees and privacy and security standards directly with the suppliers. These include OverDrive, 3M Cloud Library, Axis 360, Content Cafe, Syndetics, and Zola Books.

BiblioCommons has also entered into contracts directly with integration partners, which has allowed BiblioCommons to implement privacy security standards by agreement. Examples include LibraryThing, Zola Books, Google Analytics, FoxyCart (e-commerce payment gateway) and iDream Books.

Biblionix
Vendor response: Any integration is tightly controlled. There is no facility for "carte blanche" integration which would allow a third party to access arbitrary data. For example, there is no way for any third party to access checkout or search history at all. Patron details are available via defined protocols such as SIP, and are subject to our encryption and authentication requirements.

Ex Libris
Vendor response: Ex Libris systems run in its private cloud and no patron information is shared with external organizations or public clouds. As noted above, all interactions use HTTPS.

Questions Related to How Data Is Stored

How does your platform or system deal with the security of the storage of specific types of data?

DOES YOUR SYSTEM STORE PATRON PASSWORDS OR PINS AS UNENCRYPTED TEXT?

Auto-Graphics
Vendor response: Yes.

BiblioCommons
Vendor response: No.

Biblionix
Vendor response: Patrons' passwords are stored as salted hashes, using the bcrypt algorithm with a high computational cost. It would be impossible to derive the password from the hash.

EBSCO
Vendor response: Password storage is not currently encrypted, but is planned as an enhancement.

Ex Libris
Vendor response: Ex Libris Alma and Primo do not store patron passwords but instead authentication infrastructure makes use of integrations with the institutional identity providers systems, using standard protocols such as LDAP and SAML2.

Innovative
Vendor response: Speaking for Polaris, Virtua and Sierra, for the purpose of such integrations access is limited to the specific need rather than overly broad, and encrypted, password protected methods may be used, as described above.

OCLC
Vendor response: Patron passwords are hashed.

SirsiDynix
Vendor response: All passwords are hashed (with salt) upon entry in the system and only the hashed passwords will be used within SirsiDynix systems.

Koha
Koha stores patron passwords using a salted hash (bcrypt).

Evergreen
Evergreen currently stores patron passwords using unsalted hashes.

DOES YOUR SYSTEM STORE PATRON PASSWORDS OR PINS AS SALTED HASH OR SIMILAR MECHANISMS?

Auto-Graphics

Vendor response: No.

BiblioCommons
Vendor response: Yes.

Biblionix
Vendor response: Patrons' passwords are stored as salted hashes, using the bcrypt algorithm with a high computational cost. It would be impossible to derive the password from the hash.

EBSCO
Vendor response: User passwords are stored in plain text.

Ex Libris
Vendor response: Ex Libris Alma and Primo do not store patron passwords but instead authentication infrastructure makes use of integrations with the institutional identity providers systems, using standard protocols such as LDAP and SAML2.

Innovative
Vendor response: Speaking for Polaris, Virtua and Sierra including their respective OPACs, and Encore and Chamo discovery, none currently encrypt patron details or logs at rest, and all systems but one store PINs as salted hash or similar mechanisms. All systems' technology stacks are capable of encryption at various levels (e.g., at the database table, file, filesystem or storage subsystem level), so differences in current data at rest representation between systems are not constrained architecturally, and enablement of encryption at the filesystem or storage subsystem level would change the at rest stance of all data (logs, PINs, patron details) simultaneously for the system in question.

OCLC
Vendor response: Passwords are hashed.

SirsiDynix
Vendor response: Yes.

Koha
Koha stores patron passwords using a salted hash (bcrypt).

Evergreen
Evergreen currently stores patron passwords using unsalted hashes.

DOES YOUR SYSTEM ENCRYPT PATRON DETAILS AS THEY ARE RECORDED AND STORED?

Auto-Graphics

Vendor response: No.

BiblioCommons
Vendor response: Yes.

Biblionix
Vendor response: Yes, the entire Apollo staff interface is always encrypted via HTTPS. There is no option for the staff interface to be accessed without encryption.

EBSCO
Vendor response: EBSCO encrypts sensitive information within applications where applicable.

Ex Libris
Vendor response: Yes. All personal identifying information is stored encrypted.

OCLC
Vendor response: Passwords are hashed.

SirsiDynix
Vendor response: Yes. Note: Important distinction between hashing and encryption. While we do hash passwords for storage, database field encryption is available as a security add-on.

Koha
Patron information is not encrypted within the MySQL database.

Evergreen
Evergreen does not encrypt patron details in the database.

Security Offered in APIs

What security controls are implemented for the APIs exposed by your system? For example, do the APIs allow or require encryption in requests or responses that include patron-related data?

Auto-Graphics
Vendor response: Yes. AG requires the use of SSL as part of its API strategy as a first line of defense. Most vendors prefer the use of SSL and others don't. In either case, here are some guidelines which AG adheres to when implementing and publishing APIs with a security mindset:

1. Documentation—Reviews can be done to see exactly what the APIs should and should not do.

2. Encryption—Sensitive data always remains encrypted when not required in plain text.
3. API exchange—How to call the API, what data will be returned, format of the return and the expected error messages.
4. Authentication—Who can access the API, what information can be accessed and when resources have been accessed.
5. Authorization—Ensuring correct secondary access control post authentication like view, edit and delete requested data.
6. Black box—Unexpected inputs and requests and the validation routines.
7. Sources—Web browsers, clients and other avenues of getting to the API and their security checkpoints.

BiblioCommons
Vendor response: HTTPS is enforced for all API requests and responses.

Biblionix
Vendor response: All APIs which relate to patron data require encryption. Apollo never transmits patron data unencrypted. Also, SIP connections are secured by bidirectional keys: the client authenticates to us, and we authenticate to the client. Our only API which is unencrypted is Z39.50, since that is purely data about the collection.

EBSCO
Vendor response: EBSCO's APIs are protected in the same manner as its Web application.

Ex Libris
Vendor response: Yes. APIs are HTTPS encryption communication only.

OCLC
Vendor response: Non-public APIs only accept connections from authorized systems enforced by the encryption key and encryption for transport.

SirsiDynix
Vendor response: Encryption is not required by APIs, as some customers have requirements with which such a control would interfere. Encryption is, however, implemented by default for SirsiDynix cloud systems other than EOS, offered as a purchasable add-on for EOS, and strongly recommended to clients which host our products themselves. It is also possible to enforce encryption through the API if a customer desires.

Koha
Various Koha web services can be set up to require use of SSL.

VULNERABILITY VIA LIBRARY PROTOCOLS

Is encryption required for transactions executed through protocols such as SIP2 or NCIP?

Auto-Graphics
Vendor response: Yes. There is more than one way of handling this, but sensitive data always remains encrypted when not required in plain text.

BiblioCommons
Vendor response: Yes, when supported by the ILS.

Biblionix
Vendor response: Apollo supports SIP/SIP2 and NCIP, and follows the general principle of refusing to make any unencrypted connection.

EBSCO
Vendor response: EBSCO does not use SIP2 or NCIP to encrypt transactions. EBSCO supports HTTP/HTTPS.

Ex Libris
Vendor response: Yes. SIP2 is wrapped with an encrypted tunneling protocol to protect data in transit. NCIP is secured using HTTPS.

OCLC
Vendor response: OCLC provides the capability for encrypted transmission for SIP2 and NCIP.

SirsiDynix
Vendor response: Similarly to above, encryption is not required but is offered.

Vulnerability through APIs

What limitations to security impact your system imposed by the APIs or protocols managed by external or third-party products? Do you pass unencrypted personal data to third-party products or systems if those systems do not support encryption?

Auto-Graphics
Vendor response: External protocol security requirements have not negatively affected Auto-Graphics—in fact, they have strengthened our products by making them more robust and secure, and to some degree, more competitive in our marketplace.

We will pass unencrypted data if that is what the trading partner accepts; by the same token we will send encrypted data if that is required.

BiblioCommons
Vendor response: We've worked with third party vendors to enable encryption for all APIs where personal

data is passed. All new installs use encryption, and legacy installs are being migrated.

Biblionix
Vendor response: Apollo never transmits unencrypted patron data. We go to great lengths to work with vendors to find an acceptable solution. Only one time have we been unable to work with a third-party vendor to find an encrypted solution, in which case we refused to work with that vendor (with the blessing of the library, which appreciated us guarding their patrons' data).

One aspect of third-party interaction which could be improved is authentication of NCIP requests to ILSes, particularly from statewide ILL systems. Assuming that the ILS's NCIP responder is available over HTTPS (as Apollo's is exclusively, of course), then the connection is encrypted (very good), and the NCIP client is guaranteed to be talking to the ILS (also very good), but there are no good ways for the ILS to know that a connection is coming from an authorized party. IP address authentication is the only option. HTTPS provides such a feature by way of client certificates, and there are also other ways to achieve authentication, but no ILL implementation that we've come across supports client authentication. Statewide ILL systems need to understand the importance of bidirectional authentication in their application of NCIP.

EBSCO
Vendor response: The EDS API supports SSL/HTTPS.

In its support of ILS Integrations (EBSCO Discovery Service serving as the front end for ILS/OPAC patron empowerment features), EBSCO does not pass unencrypted Publicly Identifiable Information (PII) for individual patrons. In fact, EBSCO will rely on (and send the login request to) the customer's supported institutional Single Sign On (SSO), as in its Shibboleth or SAML IdP. The data EBSCO is using/passing back and forth is the Persistent Personal Identifier (PPID) in use for the ILS. This PPID is returned as an SSO attribute and is often anonymized from the user's ID number to a patron database record identifier.

Ex Libris
Vendor response: There is no encryption of payloads with external or third-party products that do not support encryption.

Innovative
Vendor response: Speaking for Polaris, Virtua and Sierra, APIs which handle patron data (native APIs and NCIP) allow and support encryption using industry standard methods, for example HTTPS, and through configuration when acting in the server role, can disable unencrypted access as a means of requiring encryption. The exception is the SIP2 protocol, where following common industry practice for that older protocol (SIP2 does not define an encrypted transport), and so the SIP2 implementations support only unencrypted access.

OCLC
Vendor response: OCLC never transmits patron data unencrypted across the open Internet.

SirsiDynix
Vendor response: SirsiDynix passes no personal data to third party products which do not support encryption.

Koha
A variety of service providers communicate with Koha systems using SIP2. SIP2 is inherently an insecure protocol, and with very few exceptions, typically is not operated in a secure fashion. However, these services can be secured with the addition of a VPN or SSH tunnel to the service endpoints.

Evergreen
Information about library purchases can be transmitted to materials vendors via EDIFACT EDI; not all vendors, however, require the use of an encrypted protocol such as SFTP or FTPS.

Library Security Framework?

As demonstrated by the responses to this survey, considerable variation can be seen in how each of the major products available handles security and privacy. The issues mentioned in this study are only an informal representation of the possibilities that a library might want to require of its critical technology infrastructure components. In order to provide a benchmark for libraries to understand the capabilities of their current systems and to facilitate more secure and private performance of these products, a well-defined set of recommended practices could be articulated with corresponding compliance indicators.

Vendor query: Would your company be interested in a standardized specification for the treatment of patron or financial data, similar to the way that PCI provides a compliance framework for e-commerce transactions?

Auto-Graphics
Vendor response: Yes, such a standardized specification for patron, transaction, and financial data would be welcomed. The situation currently is idiosyncratic and uneven. Having an agreed-upon standard with a solid compliance and certification mechanism would be of value.

It's important to note that any such mechanism is only as strong as the weakest trading partner. If this sort of specification were to be developed, it would need to include rigorous compliance and testing mechanisms, for ILS systems, third party providers,

financial providers, and any others in the industry that work with patron and library data.

Further, such a standard should require compliance by a date certain, again, because the safety and security of patron data should be considered a high and near-term priority for all parties.

BiblioCommons
Vendor response: Yes.

Biblionix
Vendor response: Biblionix would be interested in participating in the creation of such a standard. Our concern would be the difficulty of creating a standard which accounted for all possibilities of data leakage, and then compliance with a weak standard being used as an excuse for "good enough" security by vendors. But it's almost certain that even that would be a huge step up from the state of the industry today.

EBSCO
Vendor response: Yes.

Ex Libris
Vendor response: Yes, Ex Libris security team is always interested in new standardized specifications and ongoing security improvements.

Innovative
Vendor response: In my 2014 response, I wrote that this question would likely require more of a conversation before I could respond, and my thinking is the same today. There is still uncertainty around patron data security today, of course, and a standard would bring some helpful clarity, but thinking of not just PCI but other standards including HIPPA, SoX, FERPA and others, any such standard would not seem to be a simple one, and would necessarily have overlap with similar standardization efforts outside our industry.

OCLC
Vendor response: Yes.

SirsiDynix
Vendor response: SirsiDynix would be interested in the industry adoption of well-established standards such as the U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and/or International Organization for Standardization (ISO) 27001 standards. Should industry participants determine that such standards are not usable, SirsiDynix would of course be interested in assisting with the development of such a standard; this would be with the understanding that the creation and management of a security standard by an organization that does not specialize in security brings with it liability should adopters be breached.

Koha
The Koha project would be willing to consider such specifications and/or participate in their development provided that they were publicly available under liberal license terms.

Evergreen
The Evergreen community would be open to using such a specification and/or participating in the design of such a specification, provided that the specification itself was available under liberal licensing terms.

Observations

The responses given by this selection of vendors and developers of the major automation products in use in libraries today do not reveal any significant problems or omissions in the way that they handle security and privacy. Each product has the potential to be configured in a way to reasonably protect patron privacy, and all follow general industry practices for overall system security.

As has been emphasized in this report, delivering web-based services via encrypted HTTPS transmission results in a very high level of protection for the privacy of patron search, selection, and reading behaviors. Delivering these services as clear text through HTTP exposes these behaviors to anyone with the capability to eavesdrop on the network. While not a panacea for privacy, enabling HTTPS for web-based services greatly enhances patron privacy.

All of the products in the survey have the capability to operate with HTTPS enabled. Only a few are delivered with HTTPS as the mandatory method of operation. The discovery products with mandatory HTTPS covered in this survey are:

- BiblioCore from BiblioCommons
- Apollo from Biblionix
- WorldCat Discovery Service from OCLC

These products operate only with encryption enabled through HTTPS. If the browser is directed to the HTTP form of the link, it is automatically redirected to HTTPS. This model of delivery can be considered the most desirable from a patron privacy standpoint. It is not accidental that each of these products is delivered via a multi-tenant platform. This architecture where all of the organizations using the product share the same codebase gives the provider the level of control needed to uniformly deploy a specific feature or security option.

All of the other discovery products have the capability to operate with HTTPS, but it is at the discretion of the library to enable it. These products are:

- VERSO from Auto-Graphics
- EBSCO Discovery Service from EBSCO Information Services
- Primo and Primo Central from Ex Libris
- WorldCat Local from OCLC (Delivers pages for sign-in or those that contain personal information via HTTPS, but all other pages are transmitted with HTTP, with no option for encryption.)
- Enterprise, the premium discovery interface from SirsiDynix (Can be operated with either HTTPS or HTTP. The legacy online catalogs eLibrary [previously known as iBistro or iLink] and Hip have the technical capability to use HTTPS, but I have not yet encountered examples.)
- Koha and Evergreen (Can both be set to use HTTPS, but its selective or comprehensive use requires intervention of local system administrators or implementors.)

The theoretical possibility of operating these products securely has not resulted in a broad level of implementation. I observe that most library catalogs based on these products have not been configured to operate via HTTPS. The data gathered in chapter 3 of this report confirms this trend among the largest academic and public libraries.

The resource management systems used by library personnel use encryption for their staff interfaces since these systems routinely manage sensitive data, including patron records and financial information.

Resource management products that mandate operation with HTTPS again correspond to those delivered through a multi-tenant platform:

- Alma from Ex Libris
- WorldShare Management Services from OCLC
- Apollo from Biblionix
- BLUEcloud staff modules from SirsiDynix

All of the other products can be configured to use HTTPS. Since these products are used only by authorized staff of the library, it was not possible to make observations regarding the frequency with which secure communications are implemented among the libraries that have implemented these products.

For both the patron and staff products that lack mandatory deployment of HTTPS, the configuration options are usually all or nothing. This approach makes it easier for a library to shift to secure deployment than having to select specific pages or resources. Selective use of encryption was a desirable approach in the time when the use of encryption to support HTTPS consumed significantly more computational resources than HTTP. With the current generation of web server infrastructure components, enabling HTTPS requires only a minimal increase in resources.

The responses to the questionnaire also reveal generally sound practices for password management and overall system security. Most of the products follow the industry standard of not storing passwords directly, but only the derived salted hash. Patron details tend to be stored in operational databases and may not be encrypted. It is more common for log files to be anonymized, and no vendors reported routine encryption. Biblionix, consistent with its attention to security details, reports that Apollo encrypts log entries as well as circulation and search data.

In the event of a root-level security intrusion, these systems would likely not be able to prevent access to general patron details, but patron and staff passwords would not be easily compromised. Access to logs in a way that would reveal patron-identifiable search, selection, and reading behaviors would not be possible. OCLC reports that its logs minimize attribution, and EBSCO does not specifically report that its logs are anonymized but are protected through the security controls of its commercial logging device.

Overall, this study reveals an uneven reality in the way that these products protect patron privacy. Those of recent vintage that follow modern architectures provide the highest level of privacy through mandatory encryption. Legacy products include the capability for secure operation, but leave it at the discretion and initiative of the library. Especially for products implemented locally, the library may or may not have the expertise to install and manage the needed certificates and security configuration options. Some of these installations may rely on outdated versions of the products and hardware approaching end of life and may be considered too fragile to reconfigure. The server-oriented systems hosted by the vendor likewise have not been implemented with security enabled consistently.

Chapter 3

Data from Library Implementations

In order to assess the current state of practice in the way that libraries handle patron privacy, observations were made for a selection of libraries. The two groups selected for the study included the members of the Association of Research Libraries and the largest 25 public libraries in the United States. The selection of these two groups focuses the study toward the largest and most sophisticated libraries. These libraries are more likely to have the technical capacity and the financial resources to implement products that meet a high level of functional requirements. Smaller libraries may have fewer resources to configure or adjust their technology products relative to privacy concerns. This exercise hypothesized that these groups of libraries would exhibit the most sophistication in their websites and catalogs, both in terms of features and in attention to privacy and security.

Methodology

The study relies on lists of libraries belonging to the two groups of interest. The members of the Association of Research Libraries are listed on the organization's website, and a list can be generated from the libraries.org resource on Library Technology Guides.

Association of Research Libraries
www.arl.org

Libraries.org resource
http://librarytechnology.org/libraries/arl
or
http://librarytechnology.org/libraries./search.pl?ARL=on

The list of the largest 25 public libraries in the United States was based on the ALA Fact Sheet, "The Nation's Largest Public Libraries: Top 25 Rankings."[1] An expanded version of the ranking table, provided in table 3.1, includes the integrated library system and online catalog product implemented by each organization.

Each of the websites in the two lists was visited in the last week of December 2014, noting several characteristics:

- Is the website itself delivered using HTTP or HTTPS?
- What is the primary discovery interface or online catalog presented? Many of the ARL libraries feature both a discovery interface and a traditional online catalog. Some have multiple discovery interfaces, though the one presented as the default search tool is the one considered. These public libraries generally do not have article-level discovery services, so only the online catalog was considered.
- Does the discovery interface use HTTPS by default?
- Does the online catalog use HTTPS by default?
- Using the Ghostery plug-in for Chrome, all tracking mechanisms detected on the website, online catalog, or discovery interface were noted. The following notation can be seen on tables 3.2 and 3.3. (Abridged forms of the tables appear here; the full tables are available online.)
  - a = all major components, including website, catalog, and discovery interface
  - d = discovery interface only
  - c = online catalog only
  - w = website only

Ghostery plug-in for Chrome
https://www.ghostery.com

A variety of tracking mechanisms were noted. Most, if not all, send some data to an external organization. Whether that data includes personally identifiable information would require additional technical analysis and tracing. At a minimum, these tracking mechanisms report externally that a specific resource or page associated with the specific web server was accessed at a specific time.

- Google Analytics
- Google Ajax search API
- Google AdSense
- Google Translate
- Google Tag Manager
- DoubleClick (owned by Google)
- Yahoo Analytics
- Adobe Omniture Analytics
- Adobe Tag Manager
- Adobe TypeKit
- Facebook Connect
- Facebook Social Plugin
- Twitter Button
- AdThis
- Piwik Analytics
- Crazy Egg
- WebTrends
- New Relic

Observations

Data collection for this study was performed in November and December 2015, with all data reviewed and revised in the last week of December. The data collected is meant to represent only a snapshot reflecting current practices at that specific time. It is expected that many of the sites may change even by the time this report is published. This data can also serve as a baseline to measure any changes that might take place in the future. Any such changes would serve as a barometer of whether the concerns related to patron privacy increase or diminish, at least as measured by the implementation of secure resource delivery and through the use of tagging mechanisms related to external commercial entities.

Large Academic Libraries

- Out of 124 ARL member libraries considered, only 16 (13%) present their main website using HTTPS.
- Out of the 95 ARL member libraries that feature an online catalog search on their website, only 12 (14%) default to HTTPS for search activity.

Table 3.1. The 25 largest US public libraries, included in this study

Los Angeles Public Library, CA
New York Public Library
County of Los Angeles Public Library, CA
Chicago Public Library, IL
Brooklyn Public Library, NY
Queens Borough Public Library, NY
Miami-Dade Public Library System, FL
Houston Public Library, TX
Harris County Public Library, TX
Broward County Libraries Division, FL
San Antonio Public Library, TX
Orange County Public Libraries, CA
Free Library of Philadelphia, PA
Phoenix Public Library, AZ
Las Vegas-Clark County Library District, NV
Hawaii State Public Library System, HI
King County Library System, WA
Sacramento Public Library, CA
San Diego Public Library, CA
Hillsborough County Public Library Cooperative, FL
Dallas Public Library, TX
San Bernardino County Library, CA
Riverside County Library System, CA
Hennepin County Library, MN
Orange County Library District, FL

- Out of the 100 ARL member libraries that feature a discovery service on their website, only 17 (17%) default to HTTPS for search activity.
- Out of 124 ARL member libraries considered
  - All 124 included some form of tracking tag to an external commercial entity.
  - 119 include Google Analytics page tagging on their main website.
  - 11 include Google AdSense advertising tracking tags on their main website or discovery interface.
  - 22 include DoubleClick advertising tracking tags on their main website or discovery interface.
  - 37 include New Relic tags on their discovery interface. ProQuest Summon consistently embeds New Relic.

Large Public Libraries

- Out of the 25 large public libraries considered, only 2 (8%) present their main website using HTTPS.
- Out of the 25 large public libraries considered, only 7 (28%) use HTTPS by default for catalog search activity.
- Of these 7 secure catalogs, 5 base their catalog search on BiblioCore.
- 24 out of the 25 (96%) embed Google Analytics tags for their website and catalog.

Table 3.2. This table shows data from the largest public libraries on the security of their catalog and website, as well as whether Google Analytics is in place. This is an abridged form of the larger table, reviewing the use of other analytics tools, available from the Library Technology Guides website. http://librarytechnology.org/web/breeding/ltr-52-4-table3-2

	Website	Catalog	Secure?	Google Analytics
Los Angeles Public Library, CA	n	LS2 PAC	n	wc
New York Public Library	n	Encore	n	wc
County of Los Angeles Public Library, CA	n	eLibrary	n	wc
Chicago Public Library, IL	n	BiblioCommons	y	wc
Brooklyn Public Library, NY	n	BiblioCommons	y	wc
Queens Borough Public Library, NY	n	Local	n	wc
Miami-Dade Public Library System, FL	n	PowerPAC	n	wc
Houston Public Library, TX	n	Portfolio	n	wc
Harris County Public Library, TX	n	Portfolio	n	wc
Broward County Libraries Division, FL	n	LS2 Pac	n	wc
San Antonio Public Library, TX	n	WebPac Pro	n	wc
Orange County Public Libraries, CA	n	Enterprise	y	wc
Free Library of Philadelphia, PA	n	VuFind	y	wc
Phoenix Public Library, AZ	y	PowerPAC	n	wc
Las Vegas-Clark County Library District, NV	n	WebPac Pro	n	wc
Hawaii State Public Library System, HI	n	Enterprise	n	wc
King County Library System, WA	n	BiblioCommons	y	wc
Sacramento Public Library, CA	y	Encore	n	wc
San Diego Public Library, CA	n	BiblioCommons	y	wc
Hillsborough County Public Library Cooperative, FL	n	PowerPAC	n	wc
Dallas Public Library, TX	n	PowerPAC	n	wc
San Bernardino County Library, CA	n	PowerPAC	n	w
Riverside County Library System, CA	n	Powerpac	n	wc
Hennepin County Library, MN	n	Local?	y	wc
Orange County Library District, FL	n	WebPac Pro	n	

w = website
c = catalog

- 4 out of the 25 embed DoubleClick advertising tracking tag.
- 1 out of the 25 embeds Google AdSense advertising tracking tag.
- 7 embed Facebook Connect.

The results of this study are nothing short of alarming relative to the privacy practices seen in these elite groups of institutions. Despite the findings in chapter 2 that all of the systems available have the technical capacity to be deployed using encrypted secure communications, only small percentages of these libraries have implemented it for their online catalogs or discovery services. Almost as few implement their websites with security, which is also standard capability of commercial and open-source web servers or content management systems. These sites are also promiscuous in their use of commercial tracking agents. Almost all use Google Analytics. Only one site, the University of Albany, was observed with no detectible tracking agents. The use of commercial advertising tracking agents from Google AdSense and DoubleClick is also noteworthy.

It should also be noted that the major commercial services and social networks employ HTTPS, including Facebook, Twitter, and all Google services.

The lack of pervasive implementation of secure communications use cannot be blamed on the lack of capability in the systems, but rather may be attributed only to gaps in awareness of its benefits or lack of expertise to reconfigure existing implementations. Vendors and libraries could partner to reshape the security landscape quickly if this were identified as a priority.

The public exposure of network traffic can be considered as only one small component of an overall strategy in the way that technology systems used in a library environment protect patron privacy. How technology infrastructure handles patron data and search behaviors can be seen as the foundation needed to support higher-level features and services that may also have privacy implications. Libraries may, for example, want to provide social features that enable their patrons to opt into sharing information about themselves and their reading habits, either with selected groups of other patrons or publicly. Libraries might want to collect additional

Table 3.3. This table, running multiple pages in its full form, shows security findings from each ARL library's website, catalog, and discovery service, along with use of Google Analytics. The full data set showing all analytics tools found can be downloaded from the Library Technology Guides website. http://librarytechnology.org/web/breeding/ltr-52-4-table3-3/

	Website	Catalog	Secure?	Discovery Interface	Discovery Secure?	Google Analytics
Arizona State University	y	WebPac Pro	n	Summon	y	a
Auburn University Libraries	n	VuFind	n	none		a
Boston College	n			Primo	n	a
Boston University	n			Primo	n	a
Boston Public Library	n			BiblioCommons	y	a
Brigham Young University	n	eLibrary	n	Local	y	a
Brown University	n	Blacklight	y	Summon	y	a
Case Western Reserve University	n	WebPac Pro	n	Summon	n	a
Center for Research Libraries	n	WebPac Pro	n			a
Colorado State University	n			VuFind	n	a
Columbia University	n			Blacklight		a
Cornell University	y			Blacklight	y	a
Dartmouth College	n	WebPac Pro	n	Summon	n	a
Duke University	n	Aleph	n	Drupal/ Summon		a
Emory University	n			Primo	n	a
Florida State University	y	Mango	n	Summon	n	a
George Washington University	n	Drupal	n	Drupal/ Summon	n	a
Georgetown University	n	WebPac Pro	n	Summon	n	a
Georgia Institute of Technology	n			Primo	n	w
Harvard University	n	Aleph	n	Primo	n	w
Howard University	n	WebVoyage	n	Summon	n	dc
Indiana University	y	Blacklight	n	Drupal EDS API	y	a
Iowa State University	n			Primo	n	a
Johns Hopkins University	n	Blacklight	y	Blacklight	y	a
Kent State University	n	WebPac Pro	n	EDS	n	a
Louisiana State University	n	eLibrary	n	EDS	n	a
Massachusetts Institute of Technology	n	EDS	y	EDS	y	a
McGill University	n	Aleph	n	WorldCat	n	a
McMaster University	n			VuFind	n	a
Michigan State University	n	WebPac Pro	n	Summon	n	a
National Archives and Records Administration	n					w
National Research Council Canada	n	WebPac Pro	n			a
New York State Library	n					a
New York University	n	Primo	n	Xerxes / EDS	y	a
New York Public Library	n	Encore	n			a
North Carolina State University	n			Local	n	a
Northwestern University	n			Primo	n	a
Ohio State University	y	WebPac Pro	n	Worldcat	n	a
Oklahoma State University	n	Primo	n	Summon	n	a
Pennsylvania State University	y			Summon	y	a
Princeton University	n			Blacklight/ Primo	n	a
Purdue University	y			Primo	n	a
Queen's University	n	WebVoyage	y	Summon	n	a
Rice University	n	eLibrary	n	Drupal EDS API	n	a

Table 3.3. (cont.)

	Website	Catalog	Secure?	Discovery Interface	Discovery Secure?	Google Analytics
Rutgers University	n	VuFind	y	EDS		a
Smithsonian Institution	n	iPac	n	Summon	n	a
Southern Illinois University	n	VuFind	y	EDS	?	a
Stony Brook University	n	Aleph	n	EDS	n	a
Syracuse University	n	WebVoyage	n	Summon	n	a
Temple University	n	WebPac Pro	y	Summon	n	a
Texas A&M University	n	WebVoyage	n	EDS		a
Texas Tech University	n	Primo	n	EDS	n	a
Tulane University	n	WebVoyage	n	Primo	n	a
Library of Congress	n	Local	n			
National Agricultural Library	n	Voyager	n			a
National Library of Medicine	y	Voyager	n	PubMed	n	
Universite Laval	n			Ariane	n	a
University at Albany	n	Aleph	n	EDS		
University at Buffalo	n	VuFind	n	Summon	n	a
University of Alabama	n	WebVoyage	n	Drupal EDS API	n	a
University of Alberta	n	eLibrary	n	EDS	n	a
University of Arizona	n	WebPac Pro	n	Summon	n	a
University of British Columbia	n	WebVoyage	n	Summon	n	a
University of Calgary	n			Drupal / Summon	n	a
University of California -- Berkeley	n	WebPac Pro	n	EDS	n	a
University of California -- Davis	y	Aleph	y			a
University of California -- Irvine	n	WebPac Pro	n			a
University of California -- Los Angeles	n	WebVoyage	n	Summon		a
University of California -- Riverside	n	WebPac Pro	n	EDS	n	a
University of California -- San Diego	n	WebPac Pro	n			a
University of California -- Santa Barbara	n	Aleph	n			a
University of Chicago	n	VuFind	y	EDS API		a
University of Cincinnati	n	WebPac Pro	n	Summon	n	a
University of Colorado -- Boulder	n	Encore	n			a
University of Connecticut	n			Primo	n	a
University of Delaware	n			WorldCat	n	a
University of Florida	n	Mango	n	Summon	n	a
University of Georgia	n	VuFind	n	EDS	n	a
University of Guelph	n			Primo	n	a
University of Hawaii -- Manoa	n			Primo	n	a
University of Houston	n	WebPac Pro	n	Primo	n	a
University of Illinois -- Chicago	n	VuFind	n	Summon	n	w
University of Illinois at Urbana-Champaign	n	VuFind	n	Local?	n	a
University of Iowa	n	Aleph	n	Primo	n	a
University of Kansas	y	Voyager	n	Primo	n	a
University of Kentucky	n	WebVoyage	n			a
University of Louisville	n			WorldCat	y	a
University of Manitoba	n	Primo	n	Primo	n	a
University of Maryland	n	Aleph	n	WorldCat	y	a
University of Massachusetts -- Amherst	n	Aleph	n	WorldCat	n	a
University of Miami	n	WebPac Pro	n	Summon	n	a
University of Michigan	n	VuFind	n	Drupal	n	a
University of Minnesota -- Twin Cities	y	Primo	n	Primo	n	a
University of Missouri -- Columbia	n	WebPac Pro	n	Summon		a

Table 3.3. (cont.)

	Website	Catalog	Secure?	Discovery Interface	Discovery Secure?	Google Analytics
University of Montreal	n	Primo	n	Primo	n	a
University of Nebraska -- Lincoln	n	WebPac Pro	n	Encore	n	a
University of New Mexico	n			WorldCat	y	a
University of North Carolina -- Chapel Hill	n	Endeca	n	Local	n	a
University of Notre Dame	n	Primo	n	Primo		a
University of Oklahoma	y	Primo	n	Primo	n	w
University of Oregon	n	Primo	n	Primo	n	w
University of Ottawa	n	WebPac Pro	y	Primo	n	a
University of Pennsylvania	n	Local	n	Local	n	a
University of Pittsburgh	n	Voyager	n	Summon	n	a
University of Rochester	n	WebVoyage	n	Summon	n	dc
University of Saskatchewan	n	WebPac Pro	n	Primo	n	a
University of South Carolina	n	WebPac Pro	n	Encore		a
University of Southern California	y			Summon	n	
University of Tennessee -- Knoxville	y			Primo	n	a
University of Texas -- Austin Libraries	n	WebPac Pro	n	Summon	n	a
University of Toronto	y	Local?	n	Summon API	y	a
University of Utah	n			Primo	n	a
University of Virginia	n	eLibrary	n	Blacklight	n	
University of Washington	n			Primo	n	a
University of Waterloo	n	Primo	n	Local	n	a
University of Western Ontario	n	WebPac Pro	n	Summon	n	a
University of Wisconsin -- Madison	n	Local?	y	Primo	n	a
Vanderbilt University	n	Primo	n	Local / Primo	n	a
Virginia Tech	n	WebPac Pro	n	Summon	n	a
Washington State University	n	Primo	y	Primo	y	a
Washington University in St. Louis	n	WebPac Pro	n	Metalib / Primo	n	a
Wayne State University	y	WebPac Pro	n	Local / Summon	y	a
Yale University	n	WebVoyage	n	Local	n	a
York University	n	eLibrary	n	VuFind	y	a

non-anonymized data to create value-added services. Yet, without a secure foundation, it may be difficult to manage such services without exposing more private data than intended.

This report reveals a very uneven reality as seen in library websites, catalogs, and discovery environments related to secure transmission, a baseline requirement for patron privacy, and in the leakage of data regarding visits to library resources to commercial entities. Repeating annually the data collection described in this chapter would provide an interesting measure of whether the library community concurs with the concerns raised and is able to institute the changes needed to secure their resources and contain exposure to tracking agents. The Electronic Frontier Foundation and others are working toward improving privacy on the web at large via increased adoption of HTTPS. Given the emphasis that libraries give privacy in their ethics and policies, it would be reasonable to expect them to be leaders rather than laggards in that trend.

Related Projects and Resources

NISO Consensus Framework to Support Patron Privacy

Funded through a grant from the Andrew W. Mellon Foundation, NISO conducted a participatory process to investigate issues related to the privacy and security of systems employed by libraries and to develop a set of statements addressing key topics to help inform library practices. The project included a series of virtual discussions carried out with invited participants via webinar, a two-day in-person meeting in San Francisco, and a phase of synthesizing the information

collected into a report. The project addressed perspectives of systems provided by libraries, vendors (such as integrated library systems and discovery services), and publishers. The final report, including twelve statements of "privacy principles," titled *NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)* was published December 10, 2015, and is available online from NISO.

NISO Consensus Principles on Users' Digital Privacy
www.niso.org/apps/group_public/download.php/15863/NISO%20Consensus%20Principles%20on%20Users%92%20Digital%20Privacy.pdf

Library Digital Privacy Pledge

The Library Freedom Project has launched an initiative it calls the Library Digital Privacy Pledge, soliciting libraries to commit to the delivery of their web-based resources through HTTPS. The Library Freedom Project was founded and is directed by Alison Macrina with contributions from other volunteers. The efforts of this initiative to champion the need for libraries to encrypt transmission of their web resources is consistent with the topic of this report. The Library Freedom Project received funding from the Knight Foundation News Challenge on Libraries.

Library Digital Privacy Pledge
https://libraryfreedomproject.org/ourwork/digitalprivacypledge

EFF: Let's Encrypt

The Electronic Frontier Foundation has led an initiative called Let's Encrypt, aimed at facilitating encryption on the web for all types of sites. The project provides tools to reduce the cost and effort of enabling encryption on a site, such as providing a free service, available since December 2015, to create valid digital certificates.

Let's Encrypt
https://letsencrypt.org

Note

1. "ALA Library Fact Sheet 13: The Nation's Largest Public Libraries: Top 25 Rankings," American Library Association, August 2014, www.ala.org/tools/libfactsheets/alalibraryfactsheet13.

Other Resources

American Library Association. "An Interpretation of the Library Bill of Rights, Privacy." Accessed January 10, 2016. www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

Blum, Dan. "Privacy by Design and the Online Library Environment." *Information Standards Quarterly* 26, no. 3 (Fall 2014): 4–11. www.niso.org/publications/isq/2014/v26no3/blum.

Breeding, Marshall. "Perspectives on Patron Privacy and Security." *Computers in Libraries* 35, no. 5 (June 20015): 12–14. http://librarytechnology.org/repository/item.pl?id=20831.

Mayer, Jonathan R., and John C. Mitchell. "Third-Party Web Tracking: Policy and Technology." In *Proceedings: 2012 IEEE Symposium on Security and Privacy, S&P 2012,* 413–27. Los Alamitos, CA: IEEE Computer Society, 2012. http://dx.doi.org/10.1109/SP.2012.47. Available online at https://jonathanmayer.org/papers_data/trackingsurvey12.pdf.

Noh, Younghee. "Digital Library User Privacy: Changing Librarian Viewpoints through Education." *Library Hi Tech*, 32, no. 2 (2014): 300–17. http://dx.doi.org/10.1108/LHT-08-2013-0103.

Sturges, Paul, Vincent Teng, and Ursula Iliffe. "User Privacy in the Digital Library Environment: A Matter of Concern for Information Professionals." *Library Management*, 22, no. 8/9 (2001), 364–70. http://dx.doi.org/10.1108/01435120110406309.

Library Technology REPORTS

Upcoming Issues	
July 52:5	**Improving Web Visibility** by Ted Fons
August/ September 52:6	**Knowledgebases** by Kristen Wilson
October 52:7	**Advanced Google Analytics** by Tabatha Farney

Subscribe
alatechsource.org/subscribe

Purchase single copies in the ALA Store
alastore.ala.org

alatechsource.org

ALA TechSource, a unit of the publishing department of the American Library Association