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 SirsiDynix 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.