SOCIAL LOGIN SECURITY RISK ASSESSMENT FOR MASSACHUSETTS LIBRARIES

FINAL Report

Massachusetts Libraries
BOARD OF LIBRARY COMMISSIONERS

Submitted to:

Paul J. Kissman
Library Information Systems Specialist
Massachusetts Board of Library Commissioners
98 N. Washington St., Suite 401
Boston, MA 02114

Submitted by:

JANUS Associates, Inc.

4 High Ridge Park

Stamford, CT 06905-1325

April 28, 2016

JANUS ASSOCIATES

This page left intentionally blank.

Table of Contents

Executive Summary

The Massachusetts Board of Library Commissioners (MBLC) contracted with JANUS to investigate the risks associated with using social login to sign into library services. With patron privacy a paramount concern, MBLC wished to discover whether simplified login via Facebook, Google, LinkedIn and other social platforms to library catalogs, eBook collections, databases and other services, could be accomplished safely. The risk assessment included research and investigation to help MBLC determine the impact of social login systems, processes, policies, and procedures on library operations. The North of Boston Library Exchange (NOBLE) network acted as an advisor throughout this assessment.

Having completed the assessment, JANUS concludes that the inherent intrusions into privacy that are pervasive in social networking present risks to library patrons, and that these risks can be reduced to an acceptable level but not eliminated. Libraries are not responsible for the risks that their patrons may accept for the use of social networking sites or the internet in general, but libraries do have an interest in blocking any attempt by social login providers, social networking sites or other third party web sites from collecting information about patron use of library resources. Libraries can minimize the risk of using social login sites through the following policies and practices:

- Safe software development practices.
- Vendor management and oversight.
- Careful attention to the patron registration process.
- Monitoring and enforcement of privacy policies of third party providers.
- Clear privacy notifications and acceptance policies directed to patrons during the registration process to allow patrons to understand and accept any residual risks prior to first use of the social login option.

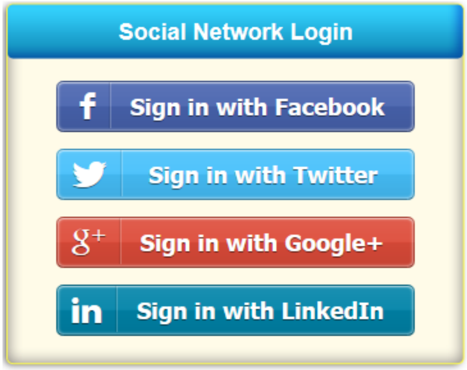
Social Login and Social Login Providers

Social login is a sign-in option that allows a user to access a website using their ID, usually an email address, and password from a social network like Facebook or Google. Social login may provide valuable benefits to the patron, by:

- Reducing the number of IDs and passwords a patron must remember.
- Improving password security by encouraging the patron to use passwords that are harder to guess.
- Giving the library patron seamless access and usage of library services.

Because social login has become a popular form of sign-in, businesses, called *social login providers*, have stepped in to fill the gap between a client organization and social networks/platforms like Facebook, Google and LinkedIn. A social login provider develops the programming to connect to a full suite of social network applications, and would minimize the programming and effort required on the part of the library networks.

Sample Social Login Buttons



Risk Assessment Process

All systems have risk. By identifying the potential risks at the start of an application development effort, mitigating strategies can be identified proactively and incorporated into subsequent phases of the project.

JANUS conducted the risk assessment with reference to the following documents: MGL Chapter 78 Section 7[1], the American Library Association's Library Bill of Rights and its Interpretation on Privacy[2] and their Privacy Toolkit. A complete list of referenced regulations and standards is included in Appendix A: Glossary.

General Risks

MBLC and NOBLE project members have an advanced understanding of, and sensitivity to, the relationships between patron privacy, technology design and project management. They understand that privacy and security of patron data will depend on application of privacy protections between the library network and social login provider. The top three privacy risks which must be mitigated are:

- HIGH RISK: Social Login Providers Are Subject to Government Information Request(s) Outside the Purview of the Commonwealth of Massachusetts – Social login providers may be incorporated or store data in states other than the Commonwealth of Massachusetts or in other countries and be governed by additional laws and regulations.
    - **Recommendation:** Frequently review social login provider policies and practices and adjust or remove library social login offerings as needed.

- MEDIUM RISK: Without Oversight, Social Login Provider Privacy Agreements May Not Be Enforced - Social login providers may issue a privacy agreement without publishing an adequate oversight program.

[1] MGL Chapter 78 Section 7 (https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXII/Chapter78/Section7)

[2] American Library Association's Library Bill of Rights and its Interpretation on Privacy (http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy) and Privacy Toolkit (http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy)

- **Recommendation:** Consider offering social login with providers that offer published third-party certifications of adherence to privacy agreements. Privacy certification programs are offered by several sources including TRUSTe, Entertainment Software Ratings Board (ESRB), and eTrust.

- MEDIUM RISK: Demographic Data May be Collected Without Adequate Patron Notification – Integration of social login code into library websites may result in patron demographic and web browsing history being collected by non-library applications, and shared with third parties without prior notification or approval of the Commonwealth library system.
  - **Recommendation:** Require the social login provider to display a library-approved notice of the potential uses of patron demographic data stating that third parties, outside of library board authority, may be able to obtain and use patron demographic and web browsing data without notifying the library system, or patron.
  - **Recommendation**: Investigate, prevent, restrict, or eliminate the ability for social login code to monitor patron activities after authentication has occurred. Prevent data leakage with secure coding practices on library network applications.

By implementing the recommended security and privacy controls, library systems may both offer the features of social login to Massachusetts library patrons and protect the privacy of patrons and security of library systems.

Social Login Providers

MBLC, NOBLE and JANUS identified a series of six requirements necessary for successful social login provider and library integration (Appendix C: LIBRARY SYSTEM REQUIREMENTS). JANUS reviewed the claims of the four major social login providers: Gigya, Janrain, OneAll, and Ping. All of the reviewed social login providers demonstrated some level of understanding regarding the library system requirements. Three common themes emerged from this analysis:

- **Library System Requirements Partially Met**: The reviewed providers offer many, but not all of the library requirements. Janrain and OneAll stand out as candidates by documenting their commitment to ensuring that their applications limit the collection of patron information at registration, and providing significantly more of the library requirements as a part of their general offering.

- **Marketing managers learn who uses the library**: After login, patron information stored on social platforms like Facebook are shared with social login providers, and may include highly detailed demographic information about people who login using this method. Privacy policies and agreements enable the social login providers to sell this information to marketing managers (and other parties with an interest in understanding who is using the social login within a certain context). Details regarding some of the information available to the provider for use or resale are listed in Appendix B.

- **MGL Ch. 78 §7 Privacy Requirements May Not Be Met:** Because social login providers are primarily aggregators and distributors of social user demographic and interest data, they do not clearly meet the MGL Chapter 78 Section 7 based criteria for protecting patron data from public disclosure.

  JANUS recommends that the library networks not disclose patron IDs or bar codes to the provider because of the resulting association of the patron identity to the user data providers collect from desktop activity and the social networks/platforms. This association would introduce a high risk to MBLC and partner networks compliance programs.

  Instead, JANUS recommends that MBLC and NOBLE consider: 1) using a system architecture that avoids disclosing patron ID to the social login provider and 2) initiating a formal secure coding process to reduce the risk of leaking information regarding patron intellectual pursuits and interests.

Introduction

MBLC is the agency of state government with the statutory authority and responsibility to organize, develop, coordinate, and improve library services throughout the Commonwealth. The Board also strives to provide every resident of the Commonwealth with full and equal access to library information resources regardless of geographic location, social or economic status, age, level of physical or intellectual ability, or cultural background.

NOBLE is a cooperative effort of 28 area libraries founded to improve library service through automation. Seventeen public library members, ten academic libraries and one special library are members of NOBLE. NOBLE was the first automated resource-sharing network in Massachusetts and the first on the Internet. Since its founding over thirty years ago, NOBLE has cost-effectively improved service to its libraries and their users through technology, in ways not possible at its inception.

JANUS is a specialty information security consulting firm that has provided independent, vendor-neutral security assessment and consulting to organizations in higher education, government, and throughout both the non-profit and private sectors for over 27 years. JANUS provides several IT consulting services including: penetration tests, audits and assessments, implementations, development, training, and information security officer services. JANUS staff is highly valued for their expertise in various security areas.

MBLC is considering supporting a social login layer in addition to direct patron sign-on to the library web services. The social login layer would allow a library patron to use an ID from a social web application to access library services. NOBLE is considering whether to act as a pilot network in implementing social login for alternative, simplified user access to its library services.

JANUS has been contracted to assist MBLC and its partner NOBLE to conduct a social login security risk assessment for library systems. The risk assessment will help the organizations to understand the impact of social login systems, processes, policies and procedures on library operation. As a result, JANUS has produced this final report and set of recommendations that describes the benefits and risks of social login for simplified access to virtual library services, as an alternative to standard credentials such as barcode/PIN or username/password.

Scope

MBLC's interest in social login is to increase availability and adoption of virtual library services. MBLC wishes to ensure that patron privacy is protected, information of patrons' library activities are not collected and aggregated with data on patron social behavior, and that third-party web monitoring tools and social networks do not obtain or distribute data on the patterns of patron library usage. In service of these objectives, MBLC directed JANUS to complete the following:

1) Participate in an initial **kickoff meeting** to discuss goals of project with MBLC and NOBLE.

2) **Identify general risks** associated with social login for libraries, severity of those risks, and ways to mitigate those risks.

3) **Identify social login service providers** that might meet the needs of the Massachusetts library community.

4) **Review claims** made by social login solution providers regarding user security and privacy. Reviewed practices and standards implemented by social login solution providers to substantiate these claims.

5) Provide a **high-level recommendation** as to whether social login is a viable solution for simplifying electronic login across Massachusetts library resources.

6) Recommend an **approach for piloting** social login integration with the NOBLE automated resource-sharing network.

7) **Identify possible issues for scaling up** to the nine automated resource-sharing networks in Massachusetts.

8) Provide a **final report**, with executive summary, outlining the findings of the project. The report will be shared with automated library networks and the library community.

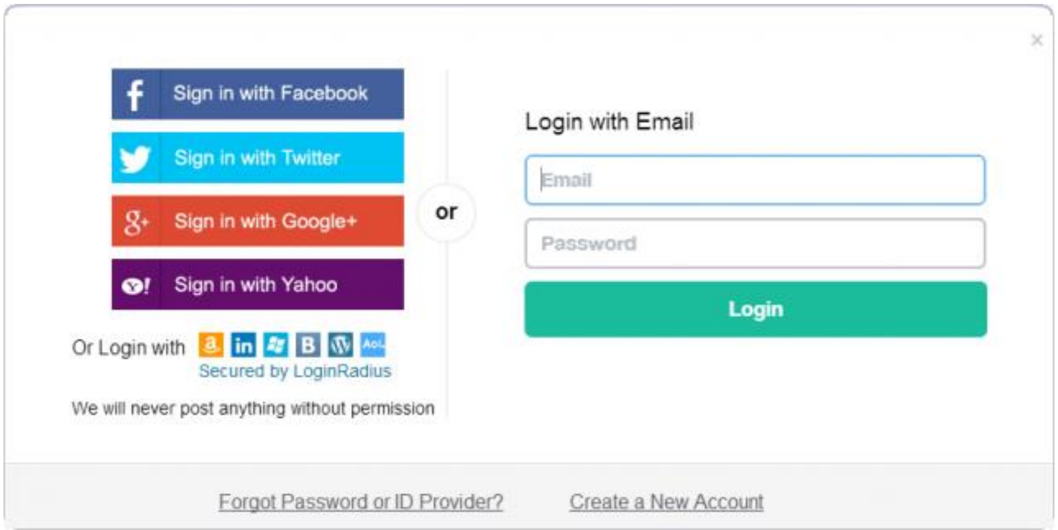
Social Login Concepts

This section introduces the basic concepts of social login in the context of a library environment.

What is Social Login?

Social login is the sign-in option that allows a user to access a website using their ID and password from a social network application like Yahoo! or Amazon. The social network for login is referred to as the social platform.

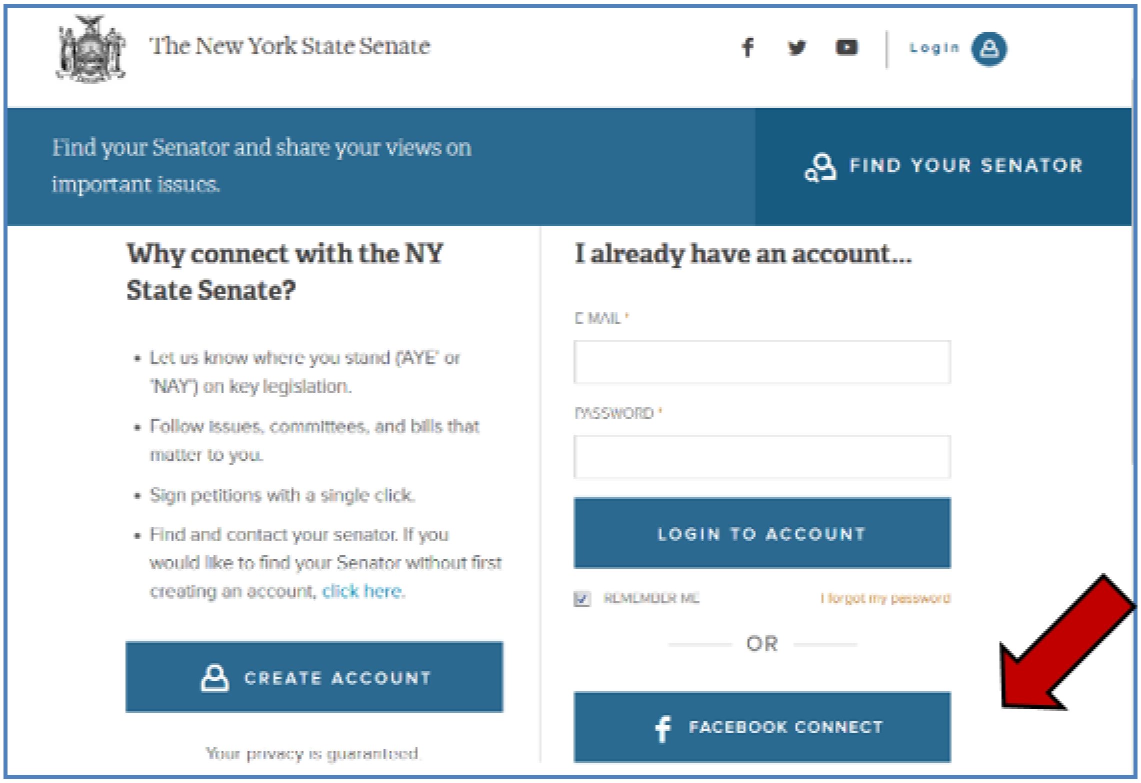
Social Login for Websites Using Google, Twitter, Facebook and Yahoo!



We will never post anything without permission

As social login gains in popularity, more organizations are offering a social login option. Social login is becoming common in both government and retail applications.

Example of social login in a government website



The New York State Senate

Login

Find your Senator and share your views on important issues.

FIND YOUR SENATOR

Why connect with the NY State Senate?

- Let us know where you stand ('AYE' or 'NAY') on key legislation.
- Follow issues, committees, and bills that matter to you.
- Sign petitions with a single click.
- Find and contact your senator. If you would like to find your Senator without first creating an account, click here.

CREATE ACCOUNT

Your privacy is guaranteed

I already have an account...

E MAIL *

PASSWORD *

LOGIN TO ACCOUNT

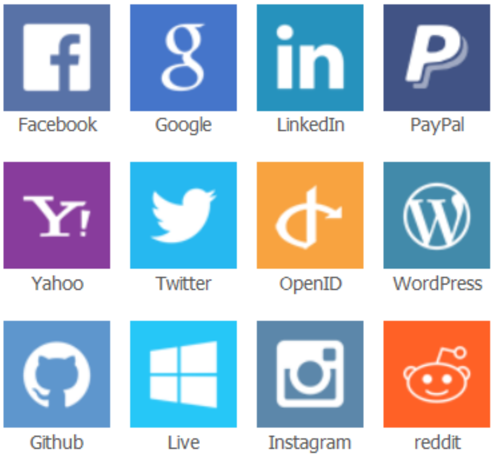
☑ REMEMBER ME I forgot my password

OR

FACEBOOK CONNECT

From the user perspective, social login is a simple sign-on option to access many online applications with only one ID and password. Social login is offered by many social networks/platforms including: Facebook, LinkedIn, Google, Twitter and Instagram.

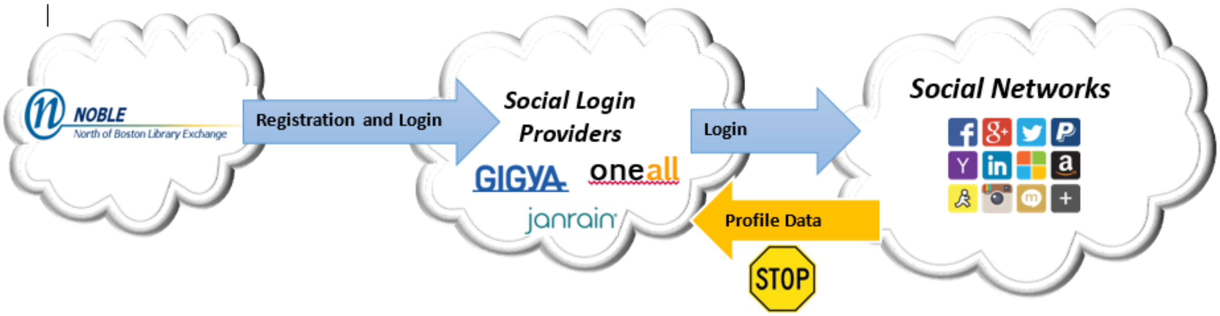
Social Login is Offered by Many Social Networks/Platforms



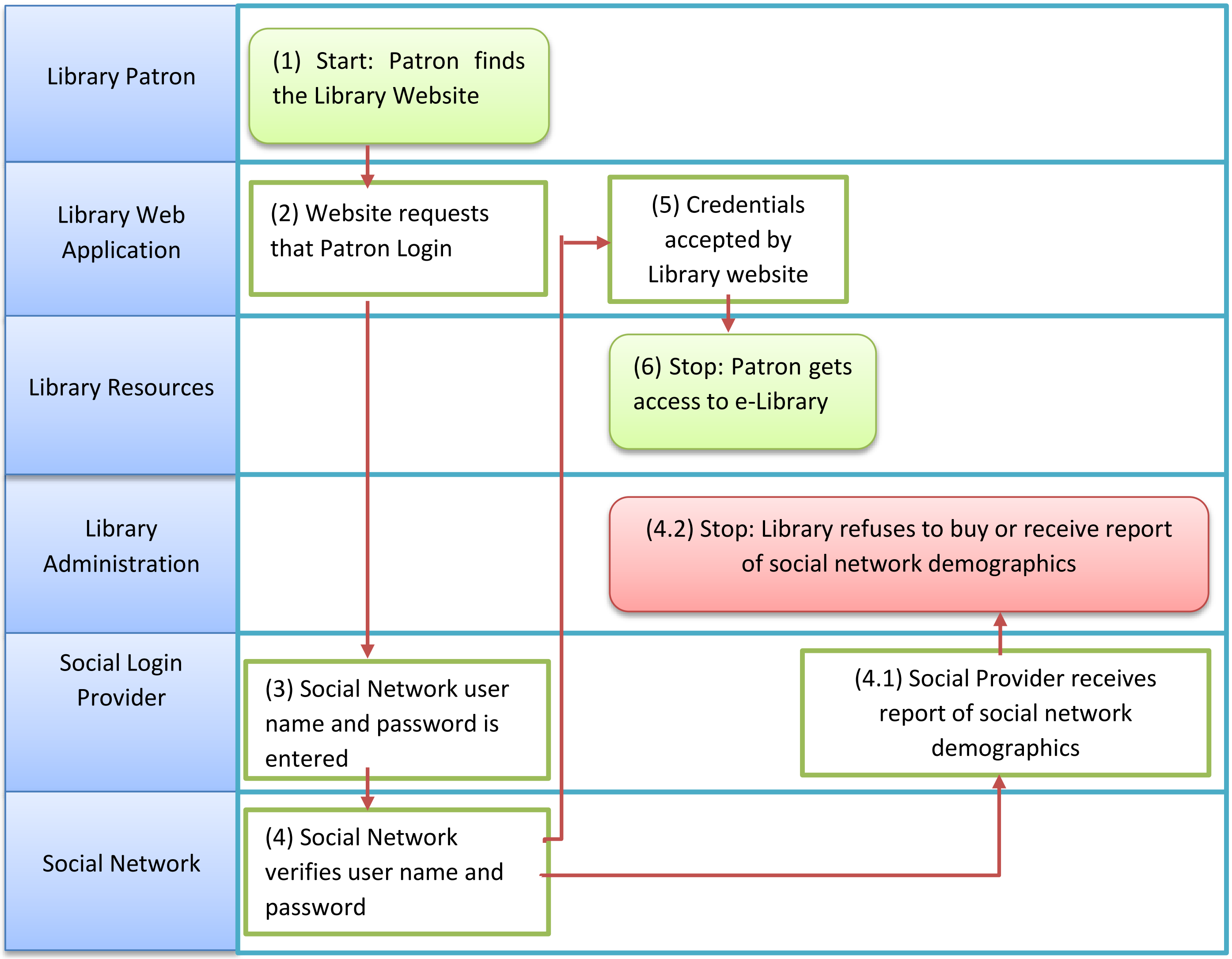
Social Login Workflow

The simplicity of the user experience relies on a complex system of interconnections to support the technology and collect the data that funds the services. In general, organizations benefit from social login because 1) the social ID option encourages user registration with easier sign-on and 2) the social network/platform data helps the organization to better understand their users as a group and as individuals. The first benefit is realized by leveraging the registration steps the user has already completed on the social network. However, the library networks will forgo the second benefit of customizing the patron experience or developing a marketing strategy based on social platform profile data, in favor of placing the highest emphasis on protection of patron privacy. The library networks will only use the social login service for registration and login. The figures below illustrate the simple form of the relationship between the library network, social login provider and social login network/platform.

Library Network Social Login: Conceptual Diagram



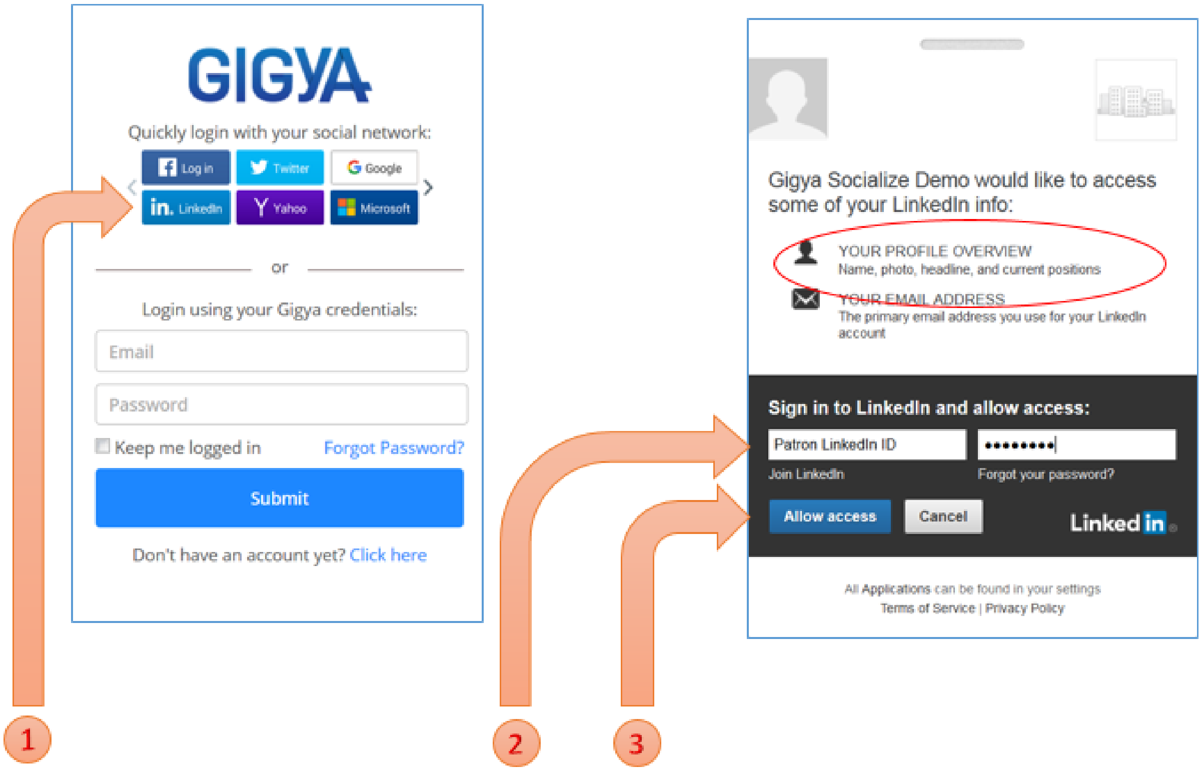
Library Social ***Login Process***


Library Patron
(1) Start: Patron finds the Library Website
Library Web Application
(2) Website requests that Patron Login
(5) Credentials accepted by Library website
Library Resources
(6) Stop: Patron gets access to e-Library
Library Administration
(4.2) Stop: Library refuses to buy or receive report of social network demographics
Social Login Provider
(3) Social Network user name and password is entered
(4.1) Social Provider receives report of social network demographics
Social Network
(4) Social Network verifies user name and password

Social Login Registration

Gigya is one of the four social login providers examined in this assessment. In the Gigya example below, registration is a three-step process:

Simple Social Login Registration Encourages User Enrollment



GIGYA

Quickly login with your social network:

or

Login using your Gigya credentials:

Email

Password

□ Keep me logged in Forgot Password?

Don't have an account yet? Click here

Gigya Socialize Demo would like to access some of your LinkedIn info:

YOUR PROFILE OVERVIEW
Name, photo, headline, and current positions

YOUR EMAIL ADDRESS
The primary email address you use for your LinkedIn account

Sign in to LinkedIn and allow access:

Patron LinkedIn ID
•••••••••

Join LinkedIn
Forgot your password?

All Applications can be found in your settings
Terms of Service | Privacy Policy

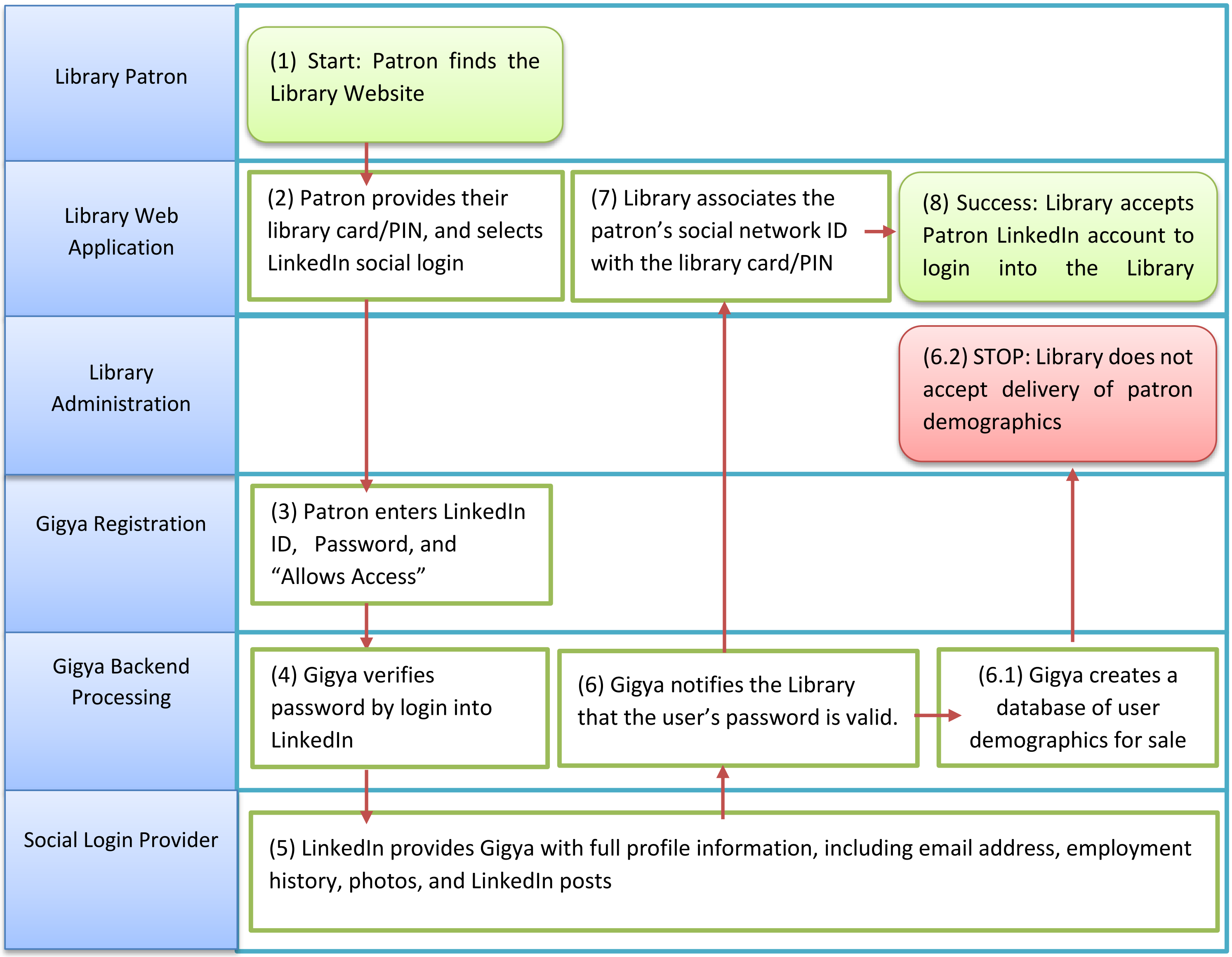
Step 1, select LinkedIn for your network;

Step 2, supply your LinkedIn ID and password;

Step 3, LinkedIn profile data (photo, name, position, and email) to be shared with Gigya. By clicking on “Allow Access”, the user is enabling Gigya to collect information from the user’s LinkedIn profile. This is a required step in order to login with this method. Gigya will then be able to collect demographic information about the individual and offer it to the library.

The registration process depicted below assumes that a recommended system architecture has been adopted, as described later in the report in section "Key Risks and Recommendations of Social Login"

Registration Process (Gigya): Swim Lane Diagram


Library Patron
Library Web Application
Library Administration
Gigya Registration
Gigya Backend Processing
Social Login Provider
(1) Start: Patron finds the Library Website
(2) Patron provides their library card/PIN, and selects LinkedIn social login
(7) Library associates the patron's social network ID with the library card/PIN
(8) Success: Library accepts Patron LinkedIn account to login into the Library
(6.2) STOP: Library does not accept delivery of patron demographics
(3) Patron enters LinkedIn ID, Password, and "Allows Access"
(4) Gigya verifies password by login into LinkedIn
(6) Gigya notifies the Library that the user's password is valid.
(6.1) Gigya creates a database of user demographics for sale
(5) LinkedIn provides Gigya with full profile information, including email address, employment history, photos, and LinkedIn posts

Benefits of Social Login

Social login has become a widely available form of user authentication to publicly available web content. Per Gartner, "Social identities can be used to simplify user registration or reduce friction in subsequent logins."[3] A valuable benefit to the user is that social login reduces the number of IDs and passwords a user must remember. From a usability standpoint, a social login is familiar to users, easy to understand, and provides the same seemless access to virtual library services as to other common web services.

Key Risks and Recommendations of Social Login

During the risk assessment, the processes from user login to data collection were examined to form a background for JANUS' recommendations regarding the risks, viability and best approach for library system social login. The risks examined in the following sections apply to both desktops and mobile (tablet or smartphone) devices. The following risk topics are presented here for further consideration.

Social Login Providers and Platforms Are Subject to Government Information Requests Outside the Purview of the Commonwealth of Massachusetts

Social login providers and platforms have participated in recent investigations regarding criminal activity. This participation will most certainly continue in the near term. Social login providers and platforms will operate in other states and internationally. Currently, library user authentication systems reside wholly in the Commonwealth. The demographic data collected related to social login could potentially reveal aspects of patron library resource usage and could potentially be subject to conflicting state and international laws.

Recommendation: To maintain compliance with MGL Chapter 78 Section 7, MBLC and NOBLE should continually review the status of the social login provider and selected platforms privacy policy and practices for changes that affect library programs.

[3] Gartner Inc. Magic Quadrant for User Authentication 1 December 2014 ID:G00260746
http://www.gartner.com/technology/reprints.do?id=1-25FOOCN&ct=141202&st=sb#dv_12_see_iam

Demographic Data May be Collected and Distributed Without Adequate Patron Agreement

Social networks are very effective at building a thorough profile of user preferences and demographics. The user data is distributed to sites that participate in social login for authentication, marketing, and personalized web pages.

Facebook represents a good example of this distribution model. Facebook defines social plugins as:

> *Tools that other websites can use to provide people with personalized and social experiences. When you interact with social plugins, you share your experiences off Facebook with your friends and others on Facebook. The Page plugin lets you easily embed and promote any Facebook Page on your website. Just like on Facebook, your visitors can like and share the Page without leaving your site.* [4]

The Facebook page plugin may display, name, photo, friend's photos, timeline and other posted information within a third-party website. If a social login widget also reveals the library website name or if unencrypted catalog activity is captured and reported with web cookies, Facebook can then use the combined activity information to know that a patron is logged on at the library and searching the catalog. As a result, Facebook could infer that a patron likes books about gardening, use catalog results as marketing information and display patron interests within the site to list bookstores nearby. This type of monitoring of user internet activity is not new, and not specifically limited to social network widgets or social login. However, every time that a social network widget is added to a web page, the capability of third parties to monitor internet usage increases.

Recommendation: This form of data collection is an inherent risk facing all internet users in the age of social networks, and is not limited to social login technology or virtual library services. To limit the scope of the marketing process, social login users can regularly clear stored cookies, and use the private mode settings available on modern web browsers that block the collection and storage of cookies and browsing history. Library systems cannot enforce these precautions on patron devices, but library services can promote and make available safety tips for safe browsing while using virtual library services.

Management of data held by the social login provider is governed by the agreement with the library system and the financial model of that social login provider. The typical design of these agreements as related privacy policies assume a different perspective on privacy than is required by libraries. For library social login, the library system would engage the provider for authentication of users but would have no interest in data aggregation and distribution of user profiles. This data collection and aggregation may occur anyway, and may be permitted by the standard agreements and privacy policies of the social login provider. Social login providers may modify their agreements without advanced warning, so that even if agreements are

[4] For further information, including coding examples, visit: http://developers.facebook.com/docs/plugins/ and http://www.facebook.com/insights/

acceptable at the time that social login is adopted, future changes to the social login provider's privacy and data sharing practices may violate the library system's standards for protection of patron privacy.

Recommendations:

- **Establish policies and procedures to approve data sharing agreements and privacy policies as a precondition of accepting the services of a social login provider. Require that these agreements be reviewed and re-approved periodically, at least once every 365 days.**
- **Make guidance available to patrons alerting them to the privacy implications of internet marketing techniques, and offering tips for protecting online privacy.**

The privacy, efficiency, and sustainability of a social login solution will depend largely on the library networks' ability to prevent data disclosure of patron identity and activity. The risk that social login providers will collect and aggregated user demographics and web browsing history cannot be entirely mitigated through privacy policies and data sharing agreements, because collecting that information is the foundation of the social login provider's business model. Libraries can take other steps to minimize the information about users that is available for discovery and collection. In addition, libraries can take this opportunity to offer guidance to patrons on safe use of the internet and social networking sites, and to raise awareness of privacy implications of data aggregation associated with internet marketing.

Recommendation: The library system can reduce the risk of unauthorized data disclosure by minimizing the amount of sensitive data in the social login provider and platform repositories. The architectural design of the library web services may be used to minimize the patron data supplied to the provider directly by 1) minimizing the transfer of patron data during login and registration and 2) securing virtual library services with encryption and secure coding practices. As an example, in NOBLE, virtual library services are age-agnostic; there are no limitations set for juvenile users. Age or birth-date should not be information required for virtual library usage. Any collection of personal information from children under 13 is subject to provisions of the Children's Online Privacy Protection Act (COPPA). Library web services should not collect or transmit personal information, including but not limited to the library patron's age. The library network should not be involved in mediating social login based on age.

System Integration of Library and Social Login Services May Reveal Library Activity to Social Login Providers

Social Login to library services requires that at some point the user's library account must be associated with the social network account. The patron's social network user name must "point to" the library patron record. A library website is then able to accept user authentication from the social network and log the correct user into the virtual library service. If, during the exchange of information required to login, the social login provider is able to collect the patron's library identification, the likelihood will increase that patron library activity will be associated with their demographic and profile information gathered from the social network. Demographic information that includes library activity may then be disseminated in ways that are out of control of the library. In order to minimize this risk, JANUS investigated four approaches to system architecture to identify those that minimized or eliminated the need to share library information about the patron with the social login provider:

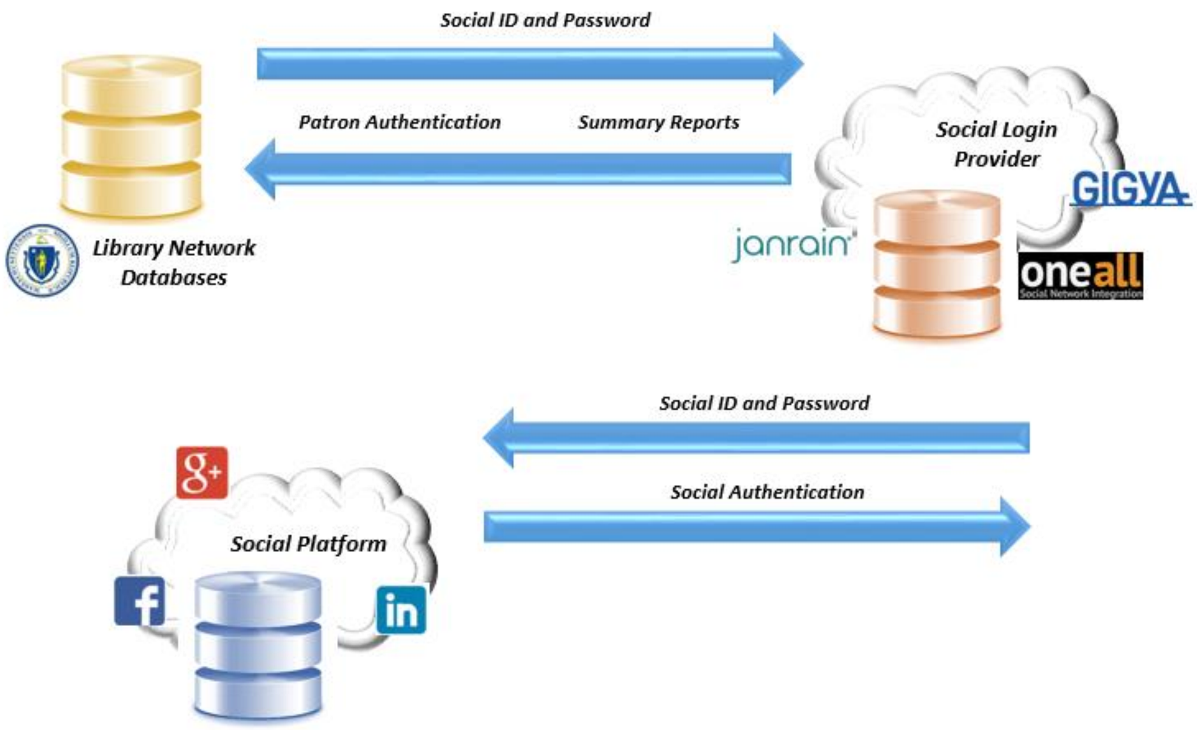
Option 1: Social Login Provider Holds Registered Patron IDs: In this scenario, user registration in social login includes the transfer of the patron ID to the social login provider. The social login provider will notify the library web application when a registered library patron logs in successfully using a social network ID. The association between the social login ID and the library patron ID is maintained by the social login provider. This option is not in compliance with MGL Ch. 78 §7.

Option 2: Social Login Provider Holds Registered Patron Tokens: In this scenario, a new identifier, in the form of a shared token, identifies the patron to both the library and the social login provider. The library maintains association between the library patron ID and the shared token. The social login provider maintains the association between the shared token and the social login ID. This option is in conformance with MGL Ch. 78 §7, but would require changes to the internal database(s) used by the library.

Option 3: Social Login Provider Perform all Authentication, including authentication for patrons who do not use social login: In this scenario, the library outsources all user authentication to the social login provider, and shares all patron IDs with the social login provider. This option is not in conformance with MGL Ch. 78 §7 and could require extensive modification of existing library systems.

Option 4: Library Network Holds Social IDs: In this scenario, the social login provider would forward to the library system the social login IDs of any user who attempted to use the virtual library system using social login. At no point would the library patron ID be shared with the social login provider. The library system would maintain the association between social login ID and library patron ID. This option is in conformance with MGL Ch. 78 §7, but would require modifications to existing library databases.

Option 4 Dataflow Diagram: Library Network Holds Registered Social IDs



Recommendation: Option 4: The architecture of library virtual services should be designed such that the library network holds social IDs: Of the options that are in conformance with MGL Ch. 78 §7, option 4 requires the least software development effort or modification of existing library systems.

Prevent Leakage of Patron Data with Secure Coding

Secure coding practices will reduce the collection of patron-sensitive data by third-parties and social platforms with web trackers, cookies and other web devices**. JANUS recommends the library system consider the following steps to protect patron privacy**:

- Use **strong encryption** on all patron identification and activity transactions to prevent marketing data collection and third-party surveillance.

- Develop and maintain **secure web services** using a recognized coding standard like Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications and Web Services.[5]

- Develop a **program of application security testing** to ensure that applications are correctly configured and free of current vulnerabilities.

Social Login Provider Claims

JANUS examined the materials presented by each of the social login providers including: policy statements, whitepapers, and software development kits. JANUS reviewed these materials for adequacy and consistency. In addition, where the provider had published names of clients, JANUS examined the client login source code to confirm consistency between the published materials and actual implementation. All of the providers reviewed demonstrated some level of understanding regarding the library system requirements.

- Although none of the social login providers were able to meet all the requirements identified by the MBLC, NOBLE and JANUS (Appendix C), both Janrain and OneAll responded quickly to information requests and demonstrated a considerable level of professional ability to communicate clearly, regarding their social offering and willingness to work with a client to meet their specific needs.

- Ping Identity sales noted that social login is still offered, but was not able to provide adequate materials for JANUS to review. Gigya, when provided with a list of similar questions, required that a non-disclosure agreement be completed prior to delivering the required information. Because Ping and Gigya have significant standing in the identity management industry and a large customer base (which could give the library system access to the most current technology and capabilities), JANUS recommends that the working group consider revisiting the discussion with Ping and Gigya to collect the remaining information.

Summary of Provider Claims Compared With Library Requirements (Appendix C)

	Tied Social Identity Basic Concerns	Account Management	Relationship Management and Decommission	Transmission Security and Protocols	Information Gathering and Storage	Platform Information Requirements
Gigya	Met	Partially Met	Partially Met	Met	Partially Met	Not Met
Janrain,	Met	Met	Partially Met	Met	Partially Met	Met
OneAll	Met	Partially Met	Partially Met	Partially Met	Met	Met
Ping Identity	Partially Met	Partially Met	Not Met	Not Met	Not Met	Not Met

[5] https://www.owasp.org/index.php/Category:OWASP_Guide_Project

Piloting Approach

JANUS recommends that NOBLE and MBLC consider taking a multi-step approach to piloting social login on the library system: 1) simple pilot with basic functionality and a security test, and 2) a full pilot with custom integration, reporting, and auditing features.

- Simple Pilot - Agree with one or more social login provider(s) on terms of a formal application security test. Demo a social login page with basic functionality.
- Full Pilot – based on a complete set of library network social login provider requirements including auditing, user management, administration, testing and service levels:
    - Consider starting the pilot by first offering it to a small group of network patrons.
    - Disclose terms of the program to the participating patrons.
    - Monitor patron information collection daily for the first 60 days of the pilot to test the data collection requirement and ensure compliance with Children's Online Privacy Protection Act (COPPA).
    - Develop a recommendation for general implementation of social login as a service enhancement based on service level reports, patron evaluations and results of the test plan.

Conclusions

Incursions into what had historically been considered private information are pervasive in social networking. Library patrons have a right to expect that virtual library resources will be protected from these incursions. Privacy risk can be reduced to an acceptable level but not eliminated. Libraries are not responsible for the risks that their patrons may accept for the use of social networking sites or the internet in general, but libraries do have an interest in blocking any attempt by social login providers, social networking sites or other third party web sites from collecting information about patron use of library resources. Libraries can minimize the risk of using social login sites through the following policies and practices:

- Safe software development practices.
- Vendor management and oversight.
- Careful attention to the patron registration process.
- Monitoring and enforcement of privacy policies of third party providers.
- Clear privacy notifications and acceptance policies direct to patrons during the registration process to allow patrons to understand and accept any residual risks prior to first use of the social login option.

Appendix A: Glossary

American Library Association's Library Bill of Rights: The American Library Association's statement of basic right entitled to library patrons

CISA - Cybersecurity Information Sharing Act of 2015[6]: Establishes terms of information sharing regarding cyber security threats between private and government entities. CISA took effect in 2016. The Department of Homeland Security issued the initial guidelines in February 2016 under the US Computer Emergency Readiness Team site regarding the Automated Indicator Sharing (AIS) initiative.[7] Rules associated with CISA will unfold throughout the coming months and discussion will continue in the public venue regarding the implementation of the law and how CISA will influence future privacy standards.

COPPA - Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505: The FTC rules that "impose certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age."[8]

ISO 27001 - International Organization for Standardization for Information Security Management Systems: A set of information security standards that may be used by an organization to establish and measure the effectiveness of an information security program.

Level of Trust - Level of Trust is defined by SANS[9] as an element of enterprise security architecture. Trust Levels are established between domains based on similar concerns for data sensitivity and security practices for data protection.

MBLC - Massachusetts Board of Library Commissioners

MGL – Massachusetts General Law

MGL Chapter 78 Section 7: Massachusetts General Law regarding the establishment and maintenance of public libraries.

NIST 800 -53 - National Institute of Standards and Technology Security Standard: Security and Privacy Controls for Federal Information Systems and Organizations.

[6] https://www.congress.gov/bill/114th-congress/senate-bill/754/text

[7] https://www.us-cert.gov/ais

[8] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[9] https://www.sans.org/reading-room/whitepapers/policyissues/approach-enterprise-security-architecture-504.

NOBLE - North of Boston Library Exchange

OWASP – The Open Web Application Security Project is a trusted source for educating the software community regarding secure coding practices. OWASP was cited in the Payment Card Industry (PCI) Data Security Standard Version 3.1, April 2015.

PIN – Personal Identification Number

Social Login Network or Platform – A service provider facilitating the development of online social connections, information sharing, and monetization of profile and demographic data. Examples are: Google, Facebook, LinkedIn, and Twitter.

Social Login Solution Provider– A technology solution company that integrates login management, and federated single-sign for multiple social networks, and provides tools such as APIs and widgets for integrating social network login with web login workflows.   Examples are: Janrain, Ping, Identity, and OneAll.

Appendix B: Social Platform Data Sharing

JANUS captured the following information from the Janrain and OneAll websites regarding social platform data.

Janrain User Data

Janrain notes that the following information that may be provided to the client by the listed social platforms after login depending on the user preferences:

- Facebook — albums, games, groups, videos
- Foursquare — type, pings, relationship
- LinkedIn — associations, patents, numRecommenders, industry, following, courses, certifications, publications, positions, jobBookmarks, honors, groupMemberships, mFeedRssUrl, skills, proposalComments, recommendations, volunteer
- Mixi — occupation, bloodType, favoriteThings
- Paypal — verifiedAccount
- SalesForce — local, userType, active

OneAll User Data

OneAll notes that, based on the user preferences, the following information may be provided to the client by the listed social platforms after login:

- Facebook — name, date of birth, gender, "about me," email, profile picture, and more
- Google — name, gender, email, profile picture, and more
- LinkedIn — name, date of birth, gender, "about me," email, profile picture, and more.

Complete information regarding OneAll connections to social platforms and data types is available at: https://www.oneall.com/services/social-login/data/

.

Appendix C: LIBRARY SYSTEM REQUIREMENTS

Tied Social Identity Basic Concerns

- To be a viable solution for the library system, the social login provider should be capable of tying social identities from the popular platforms to patron identities, have experience with clients in various industries and an established reputation in the technology. In addition, the provider must be able to support multiple protocols and interfaces to be compatible with all of the library networks web services and offer professional services, where needed, to close requirement gaps or provide implementation services.

Account Management

- Social login providers were reviewed regarding their practices and capability to manage user accounts. JANUS examined the claims of providers for managing patron data securely and in compliance with library requirements for patron privacy throughout the length of the agreement. Features that JANUS considered to support privacy and security claims included the privacy compliance program, third-party compliance reviews and limitations on the age of consumer for COPPA (Children's Online Privacy Protection Rule).

Relationship Management and Decommision

- The library system requires the social login provider with a proven method to manage relationships over time, and decommission connections as patrons leave the library system. Providers were reviewed for the ability to allow the patron to migrate from one social platform ID to another and process patron registration expiration.

Transmission Security and Protocols

- The library system requires a social login provider with the capability to deliver connectivity and messaging using secure protocols. Information was collected regarding the provider offers of OAuth2 (open standard for authorization), SAML (Security Assertion Markup Language) and encryption in transit.

Information Gathering and Storage

- The library system has strong policies regarding the information that is gathered by the social login provider, and how it is maintained. JANUS reviewed the data requirements for enrolling into the service at user registration and the protections in place to ensure the confidentiality and privacy of patron data.

Platform Information Requirements

- Finally, JANUS reviewed what, if any, patron information would be required for the provider to enroll the patron with an ID from the social platform of choice (e.g., Facebook, LinkedIn, Twitter, Google) to complete the process of enrolling a patron.

This page left intentionally blank.

End of Document