

Gardner-Webb University

Digital Commons @ Gardner-Webb University

Dover Library Faculty Professional Development
Activities

John R. Dover Memorial Library

5-19-2023

An Evaluation of the Privacy Policies of Library Vendors

Daniel W. Jolley

Gardner-Webb University, djolley@gardner-webb.edu

Follow this and additional works at: <https://digitalcommons.gardner-webb.edu/doverlibfacpub>



Part of the [Library and Information Science Commons](#), and the [Scholarship of Teaching and Learning Commons](#)

Recommended Citation

Jolley, Daniel W., "An Evaluation of the Privacy Policies of Library Vendors" (2023). *Dover Library Faculty Professional Development Activities*. 19.

<https://digitalcommons.gardner-webb.edu/doverlibfacpub/19>

This Presentation is brought to you for free and open access by the John R. Dover Memorial Library at Digital Commons @ Gardner-Webb University. It has been accepted for inclusion in Dover Library Faculty Professional Development Activities by an authorized administrator of Digital Commons @ Gardner-Webb University. For more information, please contact digitalcommons@gardner-webb.edu.

FRIDAY, MAY 19, 2023 | 3:00PM

An Evaluation of the Privacy Policies of Library Vendors

DANIEL JOLLEY

Systems Librarian

Gardner-Webb University



#nclive2023

Inspiration for the topic proposal

The Library Freedom Project posted a Vendor Privacy Scorecard back in 2018

- Analyzed the privacy policies of 12 major vendors (including ProQuest, Gale, and EBSCO)
- Analysis was based on the NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Policies) from 2015
- Assigned privacy scores (Good, Questionable, or Risky) based on 11 different questions
- No information on any type of follow-up study since 2018

Library Freedom Project / Vendor Privacy Scorecard

	Is the policy concise?	Is there contact info provided for privacy questions?	Does the privacy policy have a separate policy on cookies (not recommended)?	Who is the data being shared with?	How are vendors tracking users?	What data is being collected about users?	How long is data being kept?	How is personally identifiable information (PII) being stored? Is it encrypted?	Are there options for opting in or out?	Can users request that their data be deleted?	Can users access their PII and activity information?
Ancestry Library Online	🟡	🟡	🟡	🟡	🟡	🟡	🔴	🟢	🔴	🟡	🟡
EBSCO	🟡	🟢	🟢	🟢	🟡	🔴	🟡	🟡	🟡	🟡	🟡
Elsevier	🟡	🟡	🟡	🔴	🔴	🔴	🟡	🔴	🟡	🟡	🟡
Ex Libris	🟢	🟡	🟡	🟡	🟡	🟡	🔴	🟢	🟡	🟡	🟡
Gale Cengage	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡
JSTOR	🟡	🟢	🟡	🟡	🟡	🔴	🟡	🟡	🟢	🟡	🟢
Kanopy	🟢	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Lynda.com/LinkedIn	🔴	🟡	🔴	🟡	🔴	🟡	🟡	🔴	🔴	🟡	🟡
OCLC	🟡	🟢	🟡	🟡	🔴	🔴	🟡	🟡	🔴	🔴	🟡
Project Muse	🟢	🟢	🟡	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟡
ProQuest	🟢	🟢	🟡	🟡	🟡	🟡	🟡	🟢	🟡	🟡	🟡
Safari Books Online	🟡	🟡	🟢	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🟡

🟢 Good Privacy Practices	🟡 Questionable Privacy Practices	🔴 Risky Privacy Practices
<p>A green score denotes that the vendor approaches data collection, storage, and the management of user data from a privacy-centered standpoint. The least amount of data is being collected to reasonably use the product. All data collection is opt-in by default. Users have access to their personal and usage data and have the option to delete it. The data that is collected is not shared or sold outside of any processing that may be needed to use the vendor's services. The vendor does not use any resources to gather information about users outside of what users and their institutions have provided. A timeframe is given for when data will be deleted. The information that is collected is encrypted and provides specific information measures taken to physically protect the data. Overall, the management of user data is clearly stated and specifically outlined.</p>	<p>A yellow score denotes that it is recommended that library staff read the vendor's privacy policy carefully and proceed with caution. Vendors may be gathering more information than necessary to reasonably use the product. Users must opt-out instead of opting-in. Data about patrons may be shared or sold with other organizations and entities. The vendor may be gathering data about users from other third-party sources. There is no stated policy on when data will be deleted, or the information provided is vague. Security measures to safeguard user data are not clearly outlined.</p>	<p>A red score denotes that the vendor does not approach data collection and management from a privacy-centered standpoint. The vendor is gathering more information than necessary to reasonably use the product and some of the information may be sensitive such as health information, criminal history, documentation status, etc. Users have to opt-out instead of opt-in and opting out of sharing data may be difficult. Vendors likely do not provide users with the ability to access their user data. Users may be able to request that their personal data be deleted, yet whether the request will be fulfilled is unclear. Data about patrons is likely shared or sold with other organizations. The vendor is very likely gathering outside data about users from other third-party sources. Information may be stored indefinitely; users may, or may not, have the option to have their data deleted. The data security practice referenced in the policies are vague, and the vendors store information in other countries, which makes the data subject to the laws of those countries.</p>

Vendor Privacy Scorecard Questions

- Is the policy concise?
- Is there contact info provided for privacy questions?
- Does the privacy policy have a separate policy on cookies (not recommended)?
- Who is the data being shared with?
- How are vendors tracking users?
- What data is being collected about users?
- How long is data being kept?
- How is personally identifiable information (PII) being stored? Is it encrypted?
- Are there options for opting in or out?
- Can users request that their data be deleted?
- Can users access their PII and activity information?

Previous Studies



2010 Study by Trina J. Magi

Posed four primary questions in "A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards?"

1. Do vendors have written privacy policies?
2. Do vendors make these policies readily available to users?
3. To what degree do the existing policies meet privacy standards expressed by the information technology industry?
4. To what degree do the existing policies meet privacy standards expressed by the library profession?

2010 Study by Trina J. Magi

Used direct observation and content analysis to locate vendor policies and measure them against existing standards

- Examined 27 major library vendors
- For her formal content analysis, Magi devised a codebook of questions and worked with a non-librarian to increase reliability of analysis
- Eliminated findings where the two coders did not agree with 80% level of reliability

2010 Study by Trina J. Magi

- Broke questions into 5 categories based on the Federal Trade Commission's "Fair Information Practice Principles" of the time:
 - Notice/Awareness
 - User Choice/Consent
 - User Access/Participation
 - Data Security
 - Enforcement/Redress

Magi's Findings

- Privacy policies of library vendors failed to meet the standards of both librarians and the information technology industry in terms of protecting the privacy of user information
- Vendors were good at providing information about data collection but largely failed to give users any control over the use of their personal information
- Most vendors would share user information with third party vendors for a variety of reasons

2015 Study by April D. Lambert et al.

Posed three primary questions in “Library Patron Privacy in Jeopardy: An Analysis of the Privacy Policies of Digital Content Vendors”

1. Are digital content vendor privacy policies accessible and understandable to public library patrons?
2. Do digital content vendor privacy policies meet the standards of the library community?
3. Do these privacy policies meet other industry standards?

2015 Study by April D. Lambert et al.

Used direct observation and content analysis to locate vendor policies and measure them against existing standards

- Examined 5 major public library vendors (Axis 360, Hoopla, OneClickDigital, OverDrive, and Zinio)
- For their formal content analysis, relied on the confidential codebook provided by Magi and added several new questions of their own
- Eliminated findings where the two coders did not agree with 80% level of reliability

2015 Study by April D. Lambert et al.

- Broke questions into 5 categories based on the Federal Trade Commission's "Fair Information Practice Principles" of the time:
 - Notice/Awareness
 - User Choice/Consent
 - User Access/Participation
 - Data Security
 - Enforcement/Redress

Lambert et al.'s Findings

- Privacy policies of library vendors were much more likely to meet the privacy standards of the information technology industry than they were those of the library industry
- The reading comprehensibility of vendor privacy policies was higher than that of a significant number of public library users
- Vendors were vague when it came to defining users' rights to control their personal data, providing too little guidance and limited access rights

2022 Study by Dawn McKinnon & Clara Turp

“Are Library Vendors Doing Enough to Protect Users? A Content Analysis of Major ILS Privacy Policies”

- Focused their study on the primary Integrated Library Systems and Discovery Systems used across Canadian academic libraries
- Vendors examined were EBSCO, Ex Libris, OCLC, and SirsiDynix
- Used a modified/modernized version of the Magi coding sheet for content analysis

2022 Study by Dawn McKinnon & Clara Turp

- Delineated 24 questions used in the analysis process – I drew heavily on these 24 questions for my own set of questions
- Primarily asked Yes or No questions that allowed them to assign a score for each question (one for Yes, two for No) and an aggregate score for each of the four vendors

2022 Study by Dawn McKinnon & Clara Turp

- Broke questions into 5 broad categories:
 - Administration (contact, reviews, audits)
 - User rights
 - Data collection and retention
 - Third parties
 - Data security

McKinnon's & Turp's Findings

- Aggregate score results were very close
 - SirsiDynix – 55 (best overall score)
 - OCLC – 56
 - EBSCO – 57
 - Ex Libris – 58
- Aggregate scores do not really indicate which privacy policy is “best” but allow for an overall comparison of the vendors’ results (sometimes “No” is a better answer than “Yes” – e.g., does the vendor share data with third parties without user consent?)

McKinnon's & Turp's Findings

Recommendations to vendors for improvements:

- Review the policies regularly, and including the review schedule within the policy itself
- Allow third parties to conduct regular privacy audits on their systems and practices
- Clearly indicate the vendor's process when a security breach occurs and state detailed measures to be taken to protect user data in such a case

McKinnon's & Turp's Findings

Recommendations to vendors for improvements:

- Fully commit to keep user data private and confidential
- Increase transparency around the sharing of users' personal information with third parties

Privacy Information and Standards Sources



ALA Code of Ethics

Adopted in 1939, most recently updated in 2021

<https://www.ala.org/tools/ethics>

“3. We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.”



ALA Library Bill of Rights

Adopted in 1939, most recently updated in 2019

<https://www.ala.org/advocacy/intfreedom/librarybill>

“VII. All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people’s privacy, safeguarding all library use data, including personally identifiable information.”

Privacy: An Interpretation of the Library Bill of Rights (ALA)

Adopted in 2002, most recently updated in 2019

<https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>

“Any vendor that handles user information as part of a library’s service should have a publicly available privacy policy that commits to compliance with the *NISO Consensus Principles*. As existing contracts approach expiration, libraries should renegotiate future contracts to include these privacy safeguards.”

Resolution on the Retention of Library Usage Records (ALA)

Adopted by the Council of the American Library Association in 2006

- <https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf?sequence=1&isAllowed=y>
- Lays out ALA recommendations for all libraries in terms of protecting the privacy of patron library use

Other ALA Privacy sources

Policy Concerning Confidentiality of Personally Identifiable Information
About Library Users (adopted 1991, amended 2004)

- <https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning>

Policy on Confidentiality of Library Records (adopted 1971, last amended 1986)

- <https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconfidentiality>

Privacy Guidelines for Electronic Resources Vendors

Issued July 2002 by the International Coalition of Library Consortia (ICOLC)

- NC LIVE was part of the member group that endorsed this statement
- <https://icolc.net/statements/privacy-guidelines-electronic-resources-vendors>



[ICOLC logo. https://icolc.net/](https://icolc.net/)

Privacy Guidelines for Electronic Resources Vendors

Recommended guidelines:

- Publisher will not disclose personally identifiable information to a third party without the permission of that user (unless required by law)
- Publisher will not deny product access to any user who chooses not to allow disclosure of PII to a third party
- Publisher will post a privacy policy that is easily locatable and comprehensible

Privacy Guidelines for Electronic Resources Vendors

Recommended guidelines:

- Publisher will maintain control over its site to prevent any privacy violations from a third party
- Publisher will review the functionality of the web site regularly to ensure the privacy policy is being effectively applied
- Publisher retains the right to enforce its license terms and support user authentication by means of transferring information such as usernames or IDs to third parties

NISO Privacy Principles

NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems

- NISO is the National Information Standards Organization
- Released NISO Privacy Principles in December 2015
- <https://www.niso.org/publications/privacy-principles>

The NISO logo features the word "NISO" in a bold, dark blue sans-serif font. To the right of the text are several curved, overlapping lines in shades of blue and orange, suggesting a stylized globe or a network of connections.

NISO

[NISO logo. https://www.niso.org/](https://www.niso.org/)

NISO Privacy Principles

- Shared Privacy Responsibilities
- Transparency and Facilitating Privacy Awareness
- Security
- Data Collection and Use
- Anonymization
- Options and Informed Consent
- Sharing Data with Others
- Notification of Privacy Policies and Practices
- Supporting Anonymous Use
- Access to One's Own User Data
- Continuous Improvement
- Accountability

Other Privacy sources

North Carolina General Statutes Chapter 125. Libraries § 125-18. Definitions and Libraries § 125-1. Confidentiality of Library User Records.

IFLA Code of Ethics for Librarians and Other Information Workers (endorsed by the IFLA Governing Board in August 2012)

- <https://www.ifla.org/publications/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version/>



**International
Federation of
Library
Associations and Institutions**

[IFLA logo. https://www.ifla.org/](https://www.ifla.org/)

#nclive2023

Other Privacy sources

Fair Information Practice Principles (FIPPs)

- Released by Federal Privacy Council
- Provide guidance on the way federal government agencies uphold privacy laws
- Currently broken down into 9 basic principles
- <https://www.fpc.gov/resources/fipps/>

Other Privacy sources

Fair Information Practice Principles (FIPPs)

FAIR INFORMATION PRACTICE PRINCIPLES



Putting Together My Privacy Policy Analysis Questionnaire



Categories Based on NISO Privacy Principles

- Shared Privacy Responsibilities
- Transparency and Facilitating Privacy Awareness / Notification of Privacy Policies and Practices
- Security
- Data Collection and Use
- Options and Informed Consent / Anonymization / Supporting Anonymous Use
- Sharing Data with Others
- Access to One's Own User Data
- Continuous Improvement / Accountability

Preparing the Vendor Questionnaire

- Questions were drawn heavily from those of previous studies
- Separated each question into best-fit category
- Tried to pose Yes/No questions for the most part so that I would be able to come up with aggregate scores for the different vendors (but would include details in many question responses)
- Would combine/eliminate a few questions post-analysis (redundancy, lack of usefulness, lack of clarity, etc.)

Preparing the Vendor Questionnaire

Vendor Privacy Assessment Questionnaire

My “answers” are subjective to a significant degree

- Interpreting privacy policy language is not always easy
- Interpretations can certainly differ among different individuals
- Study would ideally include analysis by more than one person (a practice followed in the previous studies I referred to)

Preparing the Vendor Questionnaire

Did not address:

- GDPR Compliance or EU/US and Swiss-US Privacy Shield Frameworks
- Specific privacy laws in other states (e.g., California, Virginia)
- Collection of information from children
- Cookie policy details
- Privacy Policy elements outside of traditional library search/retrieval content

Vendors Included in My Analysis

- ABC-CLIO
- BiblioBoard
- Credo
- EBSCO
- Gale Cengage
- Hoopla
- Infobase
- Learning Express
- ProQuest

HeritageQuest and Newspapers.com link to Ancestry.com's privacy policy; Morningstar "protected" by Google Privacy Policy

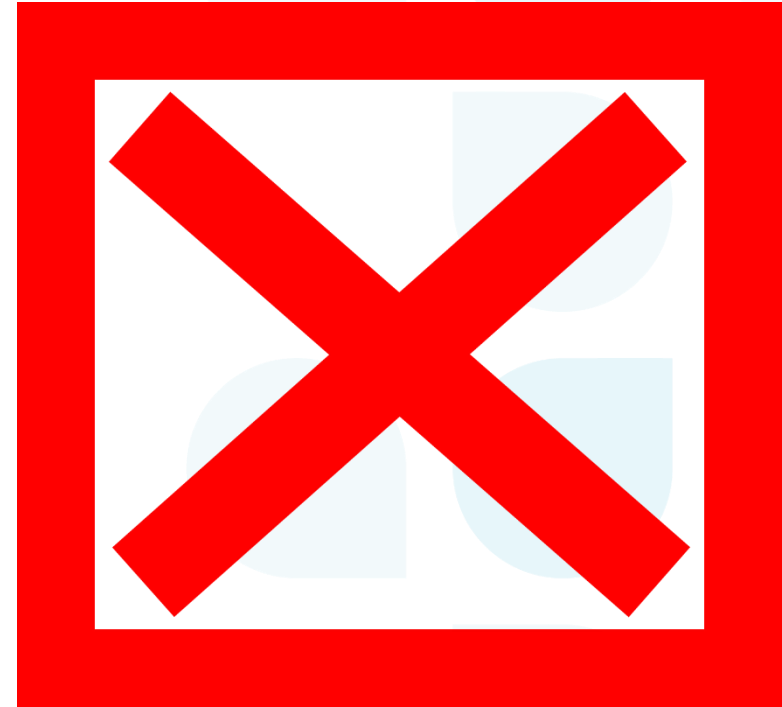
Breaking the Results Down by Category



Shared Privacy Responsibilities

Everybody strikes out

- Does the policy affirm the ALA Code of Ethics?
- Does the policy affirm any other industry- or library-related privacy standards?



Transparency and Facilitating Privacy Awareness/Notification of Privacy Policies and Practices

Is the privacy policy easy to find?

- 1 point if within two clicks

Does the policy include contact information for questions?

- 1 point for Yes

What is the date of last update?

- 1 point if updated within past 2 years

How long is the policy?

- Information only (no points assigned)

How understandable is the policy?

- Used Flesch reading ease score and Flesch-Kincaid grade level score
- 1 point if grade level of 16 or below

Transparency and Facilitating Privacy Awareness/Notification of Privacy Policies and Practices

Vendor	Category Score (Max 4)	Notes
ABC-CLIO	3	No effective date or updated date
BiblioBoard	3	Last revised in 2019
Credo	3	Last revised in 2019
EBSCO	4	
Gale Cengage	4	
Hoopla	3	Grade level score of 17.4
Infobase	4	
Learning Express	3	Grade level score of 16.3
ProQuest	4	

Transparency and Facilitating Privacy Awareness/Notification of Privacy Policies and Practices

Ease of Understanding Policy		Notes
Average length	3052 words	Ranged from 294 words (ABC-CLIO) to 4982 words (Infobase)
Average Flesch reading ease score	29	Ranged from 35.7 (BiblioBoard) [easiest to read] to 22.9 (Hoopla) [hardest to read]
Average Flesch-Kincaid grade level	15.4	Ranged from 12.5 (BiblioBoard) to 17.4 (Hoopla)

Security

Does the vendor avoid creating unnecessary personally identifiable records?

- 1 point for Yes

Does the vendor take steps to ensure the security of records?

- 1 point for Yes

Does the policy indicate that the vendor maintains full control over its site to prevent violation of privacy by a third party (such as an advertiser or ISP)?

- 1 point for Yes

Security

Within its operations, does the vendor limit access to PII to staff performing authorized functions?

- 1 point for Yes

Does the policy explicitly state that data is encrypted?

- 1 point for Yes

Security

Vendor	Category Score (Max 5)	Notes
ABC-CLIO	0	No information on security measures
BiblioBoard	4	
Credo	2	Not enough info on full control and staff access
EBSCO	3	Does not specifically mention encryption
Gale Cengage	1	Not enough info on full control and staff access; does not specifically mention encryption
Hoopla	3	No information on staff access
Infobase	4	
Learning Express	2	Not enough info on full control; does not specifically mention encryption
ProQuest	2	May hire other companies to work with data

Data Collection and Use

Does the policy explain what PII is or may be collected?

- 1 point for Yes

Does the policy state the reasons and purposes for collecting PII?

- 1 point for Yes

Does the policy indicate that the vendor does not collect any PII beyond what is necessary for the operation of the site?

- 1 point for Yes

Data Collection and Use

Vendor	Category Score (Max 3)	Notes
ABC-CLIO	2	Seems to collect more PII than necessary
BiblioBoard	3	
Credo	2	Unclear if vendor collects more PII than necessary
EBSCO	2	Seems to collect more PII than necessary
Gale Cengage	2	Seems to collect more PII than necessary
Hoopla	2	Seems to collect more PII than necessary
Infobase	2	Seems to collect more PII than necessary
Learning Express	2	Seems to collect more PII than necessary
ProQuest	2	Seems to collect more PII than necessary

Options and Informed Consent/ Anonymization/ Supporting Anonymous Use

Does the policy indicate how users can maintain their privacy (e.g., features to avoid, options to opt in or out)?

- 1 point for Yes

Are users notified of cookie policy and prompted to manage their cookie settings?

- 1 point for Yes

Does the policy state if personal data is anonymized?

- 1 point for Yes

Options and Informed Consent/ Anonymization/ Supporting Anonymous Use

Does the policy say that the providing of PII is strictly voluntary?

- 1 point for Yes

Does the policy state that the vendor will not share PII with ANY third parties (excluding agents) without the user's consent or in response to a court order?

- 1 point for Yes

Options and Informed Consent/ Anonymization/ Supporting Anonymous Use

Vendor	Category Score (Max 5)	Notes
ABC-CLIO	1	Does say that PII sharing is optional
BiblioBoard	3	User can maintain anonymity by not sharing PII; anonymizes geolocation data
Credo	0	Site usage = consent to information collection
EBSCO	1	Tells users they can opt out of emails
Gale Cengage	1	Can largely choose what PII to reveal to vendor
Hoopla	0	Site usage = consent to information collection
Infobase	1	Tells users they can disable cookies
Learning Express	0	Site usage = consent to information collection
ProQuest	2	Tells users they can opt out of providing info before disclosure; presents cookie pop-up banner at bottom of page when enter site

Sharing Data With Others

Does the vendor provide or sell PII to any third parties (excluding legal/law enforcement) ?

- 1 point for No

Does the policy delineate the reasons why the vendor would share PII with third parties?

- 1 point for Yes

Does the policy indicate that the vendor only shares anonymized and aggregated data with third parties?

- 1 point for Yes

Sharing Data With Others

Vendor	Category Score (Max 3)	Notes
ABC-CLIO	2	May share PII with third parties
BiblioBoard	2	Will only share PII for legal purposes
Credo	1	May allow third parties to use cookies to collect same info that Credo collects about you
EBSCO	1	Does not sell PII; may share some PII with partners and content providers
Gale Cengage	1	Shares PII with partners and service providers
Hoopla	1	May disclose PII with US and some non-US third parties
Infobase	1	May provide PII to partners, service providers, etc.
Learning Express	1	May provide PII to partners, service providers, etc.
ProQuest	2	Will only share PII with companies working on ProQuest's behalf who abide by ProQuest policy



Access to One's Own User Data

Does the vendor give the user the ability to view, either online or by request, the personal information collected about him/her?

- 1 point for Yes

Does the vendor give the user the ability to contest the accuracy or completeness of the personal information collected about him/her?

- 1 point for Yes

Access to One's Own User Data

Does the vendor give the user the ability to fully delete his/her personal information?

- 1 point for Yes

Does the vendor give the user the ability to remove his/her name from mailing/marketing distribution lists?

- 1 point for Yes

Access to One's Own User Data

Vendor	Category Score (Max 4)	Notes
ABC-CLIO	0	No relevant information provided
BiblioBoard	1	Will fully delete user data within 15 days of a valid request to do so
Credo	3	User can view, amend, and ask for deletion of PII
EBSCO	3	User can opt out of lists; can request changes or deletion of PII (vague on contesting accuracy)
Gale Cengage	4	Rights to edit/delete data may depend on your location (e.g., California, Virginia)
Hoopla	0	Rights seem to exist only for those in California
Infobase	2	Can unsubscribe from lists; can view and edit PII (can only delete PII if in California)
Learning Express	4	
ProQuest	4	

Continuous Improvement/Accountability

Does the vendor conduct a regular privacy audit or review of the privacy policy and procedures? How frequently? Are they conducted by an independent third party?

- 1 point for Yes

Does the policy explain how complaints and data breaches will be addressed?

- 1 point for Yes

Continuous Improvement/Accessibility

Vendor	Category Score (Max 2)	Notes
ABC-CLIO	0	No relevant information provided
BiblioBoard	2	Periodically reviewed (but no update since 2019)
Credo	2	Periodic self-assessments
EBSCO	0	No relevant information provided
Gale Cengage	0	Says the company may update the policy from time to time
Hoopla	1	Periodical evaluations; claims that company will not be liable for any damages related to failure to comply with privacy policy
Infobase	2	Internal reviews take place on a regular basis
Learning Express	0	No relevant information provided
ProQuest	1	Security reviews may include internal reviews

Total Aggregate Scores

Vendor	Category Score (Max 28)	Notes
ABC-CLIO	8	Minimalist privacy policy (294 words)
BiblioBoard	18	Weak in being transparent on user's access to own user data
Credo	13	Weak in informed consent/anonymization
EBSCO	14	Weak in informed consent/anonymization and continuous improvement/accountability
Gale Cengage	13	Weak in security, informed consent & anonymization, and continuous improvement & accountability
Hoopla	10	Strongest areas are transparency and security
Infobase	16	Weak in informed consent/anonymization & sharing of data
Learning Express	12	Weak in informed consent/anonymization and continuous improvement/accountability
ProQuest	13	Strong in user access, weak in security



Types of PII Collected

Reason	# of Vendors
Personal identifiers/contact info	9
Content interactions (searches, reading history, etc.)	7
Geolocation data	7
User posts, feedback, etc.	3

Reasons for PII Collection

Reason	# of Vendors
Provide access to services/authentication	8
Product development/improve services	6
Communicate with users	5
Marketing	4
Site security	3
Manage everyday business needs	2
Analytics	2

Reasons for Sharing PII with Third Parties

Reason	# of Vendors
Compliance with law enforcement/government; national security	8
Protect rights of company, the public, or user(s)	7
Site support and maintenance	6
Enforce license terms	5
Marketing	2
Business analysis	2
Report aggregated data to content providers	2

Conclusions & Final Thoughts

- Reading vendor privacy policies is not fun
- Privacy policies have gotten longer and more complicated in recent years
- Vendors still do a much better job of adhering to information technology industry privacy standards than library privacy standards
 - None surveyed espouse a true commitment to library privacy standards

CONCLUSIONS



[Conclusions](#), [CC BY-SA 3.0](#), via The Blue Diamond Gallery

Conclusions & Final Thoughts

- Vendors generally do a good job of detailing the PII they collect and the reasons why they collect it
- Vendors often come up short in terms of defining and describing the user's right to access his/her own data
- Most vendors claim that they will not sell or rent PII to third parties – but some will share that data with business partners that help support the site

Conclusions & Final Thoughts

- As often as not, simply using a vendor's site represents your consent to the vendor's information collection and privacy policies
- All vendors surveyed say they may release PII when asked to do so by law enforcement or government bodies
 - Only Gale Cengage implies it will only respond to subpoenas and court orders

Sources

American Library Association. (n.d.). *Library bill of rights*. <https://www.ala.org/advocacy/intfreedom/librarybill>

American Library Association. (n.d.). *Policy concerning confidentiality of personally identifiable information about library users*. <https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning>

American Library Association. (n.d.). *Policy on confidentiality of library records*.

<https://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconfidentiality>

American Library Association. (n.d.). *Privacy: An interpretation of the library bill of rights*.

<https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>

Sources

American Library Association (n.d.). *Professional ethics*. <https://www.ala.org/tools/ethics>

An Act Relating to the Confidentiality of Library User Records. N.C.S.L. 1985-486. (1985).

Federal Privacy Council. (n.d.). *Fair information practice principles (FIPPs)*. <https://www.fpc.gov/resources/fipps/>

Fiels, K. M., & Council of the American Library Association. (2006, June 28). *Resolution on the retention of library usage records*. American Library Association Institutional Repository.

<https://alair.ala.org/bitstream/handle/11213/1594/52.4.4%20Retention%20of%20Library%20Records.pdf?sequence=1&isAllowed=y>

Sources

International Coalition of Library Consortia (n.d.). *Privacy guidelines for electronic resources vendors.*

<https://icolc.net/statements/privacy-guidelines-electronic-resources-vendors>

International Federation of Library Associations and Institutions. (n.d.). *IFLA code of ethics for librarians and other information workers (full version).* <https://www.ifla.org/publications/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version/>

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors. *Proceedings of the Association for Information Science and Technology*, 52(1), 1–9.

<https://doi.org/10.1002/pra2.2015.145052010044>

Sources

Magi, T. J. (2017). A content analysis of library vendor privacy policies: Do they meet our standards? *College & Research Libraries*, 7(13), 254-272. <https://doi.org/10.5860/0710254>

McKinnon, D., & Turp, C. (2022). Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies. *The Journal of Academic Librarianship*, 48(2), 102505. <https://doi.org/10.1016/j.acalib.2022.102505>

National Information Standards Organization (n.d.). *NISO consensus principles on users' digital privacy in library, publisher, and software-provided systems (NISO privacy principles)*. <https://www.niso.org/publications/privacy-principles>

Questions?



Contact Information

Daniel Jolley

Systems Librarian

John R. Dover Memorial Library

Gardner-Webb University

djolley@gardner-webb.edu

704-406-2109

