They’re Collecting What?: Reading Vendor Privacy Policies With an Eye to Privacy Concerns

Qiana Johnson, Northwestern University & Library Freedom Institute

Nicole Becwar, Western Colorado University & Library Freedom Institute

Overview

Provide a framework to analyze vendor privacy policies.

Compare aspects of vendor policies.

Vendor privacy policy live search.

Evaluating Vendor Privacy Policies

The right to privacy – the right to read, consider, and develop ideas and beliefs free from observation or unwanted surveillance by the government or others – is the bedrock foundation for intellectual freedom. It is essential to the exercise of free speech, free thought, and free association.

ALA: Privacy http://www.ala.org/advocacy/privacy#federal

Library Freedom Project Mission:

Make real the promise of intellectual freedom in libraries.

What are some laws, best practices, regulatory agencies, and guidelines that govern patron privacy?

NISO Privacy Principles:

1. Shared Privacy Responsibilities
2. Transparency and Facilitating Privacy Awareness
3. Security
4. Data Collection and Use
5. Anonymization
6. Options and Informed Consent
7. Sharing Data with Others
8. Notification of Privacy Policies and Practices
9. Supporting Anonymous Use
10. Access to One’s Own User Data
11. Continuous Improvement
12. Accountability

Questions for Evaluating Privacy Policies

Is there a privacy policy, and how difficult is it to locate the policy on the website?

Is the privacy policy written in non-technical language that is easily understood?

Is there contact information provided for privacy questions or concerns?

Are there multiple policies in place?

How are they tracking users, and what information is being collected about users?

How long is data being kept?

How is personally identifiable information being stored (security)? Where is the data being stored (location), and is the data encrypted when at rest and in motion?

Who is the data being shared with?

Are there options for opting in or out, access the data collected on them, and can users ask that their data be deleted?

Comparison: Data Collected From Patrons

Elsevier	Kanopy	EBSCO
Name; email; postal address; username; password; phone number; password hints; educational, professional and other background info, field of study, current position; account and profile info, gender; content shared or uploaded including annotation, comments, and contributions; credit card info; questions and info sent to customer support; favorites and search queries; preferred language; frequency, type and format of alerts signed up for; institutional info and ID; information from third parties including social networks, publicly available sources, and data suppliers; IP address, browser type/version, operating system, software, "error reports & performance data," location; usage data including clickstream data, referring/exit pages, date/time stamp.	Name; institution name; email address; password; other information; messages; other information that you voluntarily provide; information about patrons from third parties including Facebook, Google (for user authentication), 3rd party business associates, publicly available sources, and affiliates, time of visit, pages visited, time spent on each page, IP address, operating system, location data (GPS coordinates) and similar information regarding patrons' devices.	Name, alias, postal address, unique personal identifier; login credentials; Internet Protocol address; email address; account name; social security number; driver's license number; passport number; person's signature; insurance policy number; education; professional affiliations; employment or employment history; bank account number, credit card number, debit card number, or any other financial information; medical information or health insurance information; browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement; geolocation data, education information.

Comparison: Who Data Is Shared With

Ancestry.com	ProQuest	EBSCO
Ancestry does not share your individual Personal Information (including your Genetic Information) with third-parties except as described in this Privacy Statement or with your additional consent. We do not voluntarily share your information with law enforcement. Also, we will not share your Genetic Information with insurance companies, employers, or third-party marketers without your express consent. **NOTE**: Ancestry does not sell your Personal Information. Ancestry may share the following categories of Personal Information about you or your use of the Services with the types of entities set forth in this section for business purposes (as defined by applicable law), or as required by applicable law: Identifiers (such as name, address, email address); Account Information (such as shipping address); Credit Card/Payment Information; Computer or Mobile Device Information; Audio and Visual information (such as recordings of calls with Ancestry Member Services or information voluntarily shared when doing consumer insights research); Inference data about you; Other Protected Classifications (such as gender and marital status); Health Information as well as Biological, Physiological, or Behavioral Traits and anything else mentioned in the table below.	ProQuest uses the information we collect for the purposes of authorizing and processing transactions, authenticating users, customer service, customer support, content processing, content classification, and providing you with information concerning the ProQuest Services. We will retain this information for as long as the customer account is active or as needed to provide the ProQuest Services, comply with our legal obligations, resolve disputes, and as needed to comply with or enforce our licenses and other agreements. We may share information—such as aggregate data and information about your use of ProQuest Services—with third parties as outlined below. We may also share the information about you in ways disclosed at the time you provide that information. ProQuest remains responsible for the personal data that we share with third parties for processing on our behalf, and we remain liable under this privacy policy if such third parties process such personal data in a manner inconsistent this privacy policy and we are responsible for the event giving rise to the damage. Please keep in mind that any information you disclose publicly – either in a Public Profile or through message boards or other public areas – may be collected and used by others, may be indexable by search engines, and might not be able to be erased from public view to the extent they have been copied to external sites. Please be careful when disclosing personal information in these public areas.	We may use the Personal Information and non-Personal Information we collect by sharing it with third-party agents, vendors, contractors, partners, or content providers of EBSCO Information Services (collectively, "Service Providers") for purposes of managing purchases of our products and services, servicing our systems, and obtaining support services for our businesses. We are not in the business of selling Personal Information to third-parties or Service Providers and will share it with Service Providers only as we describe in this Privacy Policy. In situations where we share Personal Information with Service Providers, we ensure access is granted to the Service Providers only upon the condition that the Personal Information is kept confidential and is used only for carrying out the services these Service Providers are performing for EBSCO Information Services. As part of making the determination whether we will share Personal Information with Service providers, we will obtain assurances that they will appropriately protect and maintain the confidentiality of Personal Information consistent with this Privacy Policy and as required by applicable law. The Personal Information we collect from you may be transferred to, and processed in, countries other than the country in which you live. These countries may have data protection laws that are different than the laws of your country. Specifically, the servers we use to provide our Services are located in the United States. This means that when we collect your Personal Information, we may process it in the United States or the country where you live. However, when we process your Personal Information, irrelevant of its processing location, we take appropriate measures, as discussed below, to ensure that your Personal Information remains protected in accordance with this Privacy Policy.

Comparison: User Control & Access to Their Data

Kanopy	JSTOR	Gale
Controlling Your Settings: You can limit your browser or mobile device from providing certain information by adjusting the settings in the browser, operating system or device. Please consult the documentation for the applicable browser, operating system or device for the controls available to you. You can also stop receiving promotional emails from us by following the unsubscribe instructions in those emails. Note that unsubscribe is not available for certain emails concerning your relationship or dealings with us. Do Not Track: At this time, we do not recognize "do not track" signals sent from web browsers. Third-party services that we use may collect personal information about individual users and their activities over time and across different websites. In some cases, you may be able to disable tracking mechanisms, but doing so may disable certain features of the Service. To disable tracking, please consult the documentation for your browser, operating system or mobile device. For some devices, it may not be possible to disable tracking mechanisms.	By using ITHAKA Websites, you consent to the collection and use, in accordance with this policy, of the information you provide to us. We will remove you and your personal information from our records or refrain from using your personal information in connection with certain services on request if you contact us with your request at privacy@ithaka.org. Please note that this may prevent you from accessing ITHAKA's services, including JSTOR, your personal JSTOR account, Publisher Sales Service, and certain Artstor websites and services Upon request ITHAKA will provide you with information about whether we hold any of your personal information. If you would like to review, delete or update your information, you may contact us using the contact information below. We will permit you to correct, amend, or delete information that is demonstrated to be inaccurate. We will respond to your request within a reasonable timeframe. Please note, because of the way we maintain certain services, after you delete or amend your information, residual copies may take a period of time before they are deleted from our active servers and may remain in our backup systems.	Cengage respects your rights in knowing what Personal Information we have about you and how that information is collected, used and shared. You may request we disclose what Personal Information we have and to access, make corrections to, or delete this Personal Information. You may limit the information you provide to us and also limit the communications that we send to you, such as marketing materials. Cengage complies with all laws regarding access, correction and deletion of Personal Information. At your request and where the law requires us to do so, we will confirm what Personal Information we hold about you. You may also have a legal right to obtain a copy of your Personal Information. You can make such a request by making a written request in one of the ways described in the How to Contact Us section. We may charge a processing fee for this service where permitted by law and we will require verification of the request and evidence of your identity before fulfilling your request.

Comparison: Data Retention

Kanopy	Project MUSE	Elsevier
We will retain your information as long as necessary for the purposes outlined in this Privacy Policy, and for a commercially reasonable time thereafter for backup, archival, fraud prevention or detection, or audit purposes, or as otherwise required by law.	Your information, unless otherwise specified, is stored indefinitely. However, you have the right to request that your personal information be deleted from our system. Please refer to section 4 "How to Access, Change, or Delete Your Information," for instructions. Books account information is stored for a minimum of eighteen months to facilitate credit requests related to returned books.	We retain your personal information for as long as necessary to provide the Service and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations, maintaining business and financial records, resolving disputes, maintaining security, detecting and preventing fraud and abuse, and enforcing our agreements.

Privacy Policy Live Tour

Thank you!

Qiana Johnson
Collection and Organizational Data Analysis Librarian
Assessment and Planning
Northwestern University
q-johnson@northwestern.edu

Nicole Becwar
Technical Services Librarian & Archivist
Western Colorado University
nbecwar@western.edu

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? Where?*	*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

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.

◐ Questionable Privacy Practices

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.

✗ Risky Privacy Practices

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.