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.