

Into the Breach

Using Electronic Resources Responsibly

Christina Geuther, Kansas State University Libraries

What happens when a license breach occurs at Kansas State University?

Vendor contacts Electronic Resources Librarian with details of the breach including IP address blocked and suspicious behavior

Library Information Technology Services alerts University IT Security with details to continue investigation and communicate to the alleged patron in violation

Electronic Resources Librarian notifies Library Information Technology Services to begin an investigation, as well as the Assistant Dean of Content Management and Scholarly Communication and the Head of Content Development and Acquisitions

Activity in breach of agreement is resolved and Electronic Resources Librarian officially closes case with the vendor

Helpful licensing definitions

- **Terms of Use** are conditions of a license that describe rights for interlibrary loan, scholarly sharing, and process of a search and use of content of a vendor platform or website. If a license does not specify an activity or circumstance, it is "silent" on that issue.
- **Authorized IP Ranges** register with the vendor the internet protocol address of a user's machine on a network at a campus location. There will be a different IP address for different sites of an institution in the case of multiple campuses. If a vendor sees suspicious activity occurring within the authorized IP range, it is the institution's responsibility to resolve the issue.
- **Authorized Users** are users registered with an institution as a member or affiliate with the right to access an electronic resource. Authorized Users may also include persons visiting the physical space of the library or campus.
- A **Breach** occurs when the agreement between the vendor and library is violated, which gives cause for termination.
- The **Period for Cure** is the amount of time, such as 14 days, from the vendor's contact with the library about a breach and its resolution before greater consequences such as termination or legal issues.

3 common reasons for a breach

Systematic Download

This can be manually done or through software. A systematic download is an effort to download all available content provided by a vendor's platform or website. Vendors may suspect this activity if logs show a high number of downloads or if the session length registered to an IP address is an uncharacteristically long period of time.

Unauthorized Crawling

Researchers may be interested in crawling a vendor server to process data. While in some cases this may be negotiated, it often can be considered unauthorized activity. Crawls may also come from external sources with compromised access. Without the vendor's anticipation of the crawling, the server may be significantly slowed beyond usability.

Third Party Access

Authorized users of electronic resources may be restricted to university affiliated researchers, faculty, students, and sometimes walk-ins who are within the campus authorized IP range. If an authorized user shares or a third party obtains these credentials to access an electronic resource it is against the terms of agreement.

Ways to avoid breaches

Have a Policy to Enforce

- Part of an electronic resource user policy will draw from the collection development policy used to negotiate the license. When negotiating, the licensing librarian anticipates the user population and intent for a resource on a local level. Compliance with the electronic resource user policy may become a part of the campus-wide information technology policy in order to have more consistency and acceptance by the user. A policy also gives a sense of procedure with the library and the user in the event of a breach.

Use Technology You Already Have

- EZ Proxy administrators can modify the UsageLimit to place a cap on the amount of material that may be downloaded from vendor service providers. This would discourage massive or systematic downloads, preventing a breach. Note that it may not be a solution for institutions where some electronic resources are intended for datamining.
- The discovery service interface, such as Ex Libris Primo at Kansas State University, may be customized to present some terms of use with the search result in its interface. This would help identify activities that are allowed and disallowed by the license at the user level.
- Logs on the EZ Proxy server may be used as a basis for sending warnings to users that they are reaching a limit of download activity before a vendor may suspect questionable activity and signal a breach.

Educate Limits and Opportunities to Users

- Several university libraries provide online pathfinders for using their electronic resources along with other subject guides. This is helpful to identify terms that may come into conflict for universities that negotiate for datamining in some of their electronic resource licenses but not others.
- Public Service exchanges with faculty and students can describe some of the practices that generally cause problems, such as downloading every article from one journal in a single session. They can also hear details of intended research and refer to the licensing librarian for checking the vendor's terms of use before an activity that may be regarded as suspicious.
- Note that sometimes users simply need more education about how to use a database effectively for their purposes. Rather than building a new repository to sift through the information on a personal computer, offer the opportunity to learn about what tools the vendor provides for legal use.
- If a patron has an idea for analyzing content that is not yet part of the vendor's system, some vendors agree to collaborate on enhancements.

Negotiate Revised Terms for Licensed Use

- If a university researcher caused or may cause a breach of how current terms of use are written, offer to negotiate with the vendor by offering details of the project. Similar projects like major data crawls of a vendor server may already be in place at other universities. Inform the researcher early on in their project or before it has begun so that they can include possible additional costs for this special access in their grant application. Watch how these terms are written into the license, if they are a revision applying to the whole user community or an amendment for one project and period of time in particular.

Advancing the conversation between Technical and Public Services

- At Kansas State University Libraries, few people have access to the electronic resource licenses, and they are either in Technical Services or Administration. Questions about licensed use go by referral to the Electronic Resources Librarian. Further isolating the knowledge of suspicious activities, details and identifying information are not shared beyond those conducting the investigation and communication with the user. Once brought into conversation, Public Services librarians showed great surprise and concern with the breach count over the past two years. With more librarians involved in the conversation, the broader perspective brought new ideas for a solution at the user level. The Electronic Resources Librarian and Assistant Director of Information Technology are now collaborating on research on breaches. This will be presented as a workshop for the Kansas State University Libraries Faculty and Staff.