

Privacy and Confidentiality in the Cornell University Library

The Cornell University Library believes strongly in protecting the privacy of all who use its services, in person and online. This includes your right to read anonymously. Consequently, Library staff members hold in confidence to the extent allowable by law all information about individual Library users and their choices of research or study material. Please help the Library protect your friends' and colleagues' right to privacy, and your right, by not asking staff members for this kind of information.

New York State law (N.Y.C.P.L.R. § 4509) protects the confidentiality of library records including, but not limited to, the circulation of library materials, database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, reserve requests, and the use of audiovisual materials, films, and sound recordings. Such records are to be confidential and can only be disclosed with the user's consent or in response to a subpoena, court order, or other legal requirement. Library patrons should be aware that Federal legislation (USA PATRIOT Act of 2001) has expanded the circumstances under which a federal agent may request patron records held by the Library; if such records are requested by federal authorities, the Library is prohibited by law from notifying the patron of that request. The Library forwards any law-enforcement requests for patron records to the office of the University Counsel in accordance with University Policy 4.13, [Acceptance of Legal Papers](#).

To safeguard your privacy, the Library has in place procedures that minimize instances of the retention of Library records. In addition, the Library follows relevant Cornell policies, including University Policy 4.5, [Access to Student Information](#), University Policy 4.12, [Data Stewardship and Custodianship](#), and University Policy 5.9, [Privacy of Information Technology Data](#).

Information on how the Library implements the policy outlined above is found in our description of [Library practices on the collection, use, disclosure, maintenance and protection of personally-identifiable information](#).

Library Practices on the collection, use, disclosure, maintenance and protection of personally-identifiable information

As stated in the policy on [Privacy and Confidentiality in the Cornell University Library](#), the Library believes strongly in protecting the privacy of all who use its services, in person and online. The sections below provide details about the Library's collection, use, disclosure, maintenance, and protection of personally identifiable information that you provide to us. Note that these are general principles; individual sites may have their own specific privacy policies to which links are provided. In addition, the Library also employs third party services that may have their own privacy policies. Some of these are discussed below, but you are encouraged to read the description of their privacy practices on their own web sites.

Web Sites

When you use web sites under the control of the library, certain technical information from your web browser is captured in a web activity log. This information normally includes:

- IP address
- Type and version of operating system and browser used
- Date and time of access
- Pages visited
- Search queries and result sets
- Referring URL (the web address of the page from which you followed a link to our site)

The Library uses this information to diagnose and solve problems with its services and to identify and resolve problems with computer security. Raw log files are normally maintained for 90 days for security purposes. (Two exceptions are [arXiv](#) and [Project Euclid](#), which retain complete log files permanently.) For some sites (most notably the Classic Voyager catalog), an aggregated abstract of the data is prepared each night that anonymizes session data so that searches cannot be linked to specific IP addresses or network IDs. This data is then used to analyze and improve system features.

For more information on web privacy, see CIT's [Privacy Tips for the Web](#).

Cookies and Google Analytics

Cookies are small text files that a web site uploads to your computer in order to uniquely identify your browser. Users whose computers accept cookies can store their preferences and access certain features of the web site more efficiently after the first visit. They also allow us to improve our services by better tracking how our web sites are used. You may configure your browser to disable the use of cookies. Some features of our web sites may not function properly, however, if you block the acceptance of cookies.

In 2009, in order to better understand how visitors engage with our websites, the Library began to use Google Analytics on some of its sites. Google Analytics employs first-party cookies for

data analysis, and will only use that cookie data for statistical analysis related to your browsing behavior on the Library's websites. According to Google, the data collected is anonymous and cannot be altered or retrieved by services from other domains. For more information on Google Analytics, visit [Google's web site](#). As with the library's cookies, Google Analytics can be disabled by turning off cookies in the preferences settings in your browser. Note that pages monitored with Google Analytics also contain some javascript that allows Google Analytics to track anonymously your actions on the monitored site.

For more information on cookies, see CIT's [Web Privacy Tips: Understanding "Cookies"](#).

HTTPS

When you search or browse Library web sites or databases, it is theoretically possible that someone else on the Cornell University network could "eavesdrop" on your activities (though this is a violation of Cornell University policy). This is because most data on the Internet is transmitted in clear text. One way to avoid this is to use an encrypted SSL connection using the "https" prefix. The [Classic Catalog](#) is one library system that supports HTTPS. At present, the [WordCat Local catalog](#) does not. If you are concerned that someone on the network system may be eavesdropping on your searches, use the Classic Catalog. You should be aware that even if you use an https connection, the Library cannot guarantee that submissions to our websites, any content residing on our servers, or any transmission from our servers will be completely secure.

Circulation

The Library respects the privacy of all borrowers of library materials. The Library will not reveal the names of individual borrowers nor reveal what books are, or have been, charged to any individual except as required by law. Only staff members who have a functional need to view circulation data can view who has borrowed a book.

The Library seeks to protect user privacy by purging borrowing records as soon as possible. In general, the link connecting a patron with a borrowed item is broken once the item is returned. The exception is when a bill for the item is generated. In that case, the information on who borrowed the item is retained indefinitely in our system. For security reasons, records of who requested items from the Library's special collections are also retained indefinitely.

Interlibrary Loan and Document Delivery

Interlibrary Loan lending and borrowing records have been retained since at least 2001. They are used in case there are billing problems and to comply with the record keeping requirements suggested by the CONTU (National Commission on New Technological Uses of Copyright Works) guidelines. All such records are treated confidentially. In some cases, information about requests (including the name of the requestor) is shared within the library staff for collection development purposes, but staff are instructed not to further disseminate such information. If you do not want your interlibrary loan request used for collection development purposes, you may so indicate in the "Notes" section of the request form.

The Library at times compiles aggregate data for internal business purposes and to improve Library services, but whenever this happens, all personally-identifiable information is first stripped from the requests.

Collection Development

Purchase requests and items on-order or in-process requested by patrons are linked in the catalog system to the names of users so that they can be notified when the items are ready to circulate. Such information is deemed confidential reader information and is not shared outside the Library. As noted above, collection development staff may also receive copies of Interlibrary Loan requests. Such information is used purely for internal operational purposes and is not shared outside the library.

Personalized Services

Some library services require you to provide personal information. If you are asked to provide, and do provide, personal information, the Library will explain why we ask for the information and will use such information for those specific and limited purposes. Information from other sources is not combined with that information. The Library will not sell, share, or otherwise distribute your personal data to third parties without your consent.

Reference Inquiries

You may ask questions of library staff by phone, mail, text, email, IM, and in person. All such inquiries are treated as confidential. Depending on the library unit, paper records with patron identifications may be kept for a few months or indefinitely. Information on the privacy and confidentiality of the “chat” service is found at <http://www.library.cornell.edu/ask/chatissues>. Reference questions may be posted to the [Ask a Librarian](#) blog, but only with the permission of the person asking the questions and only with all personal information removed.

Licensed Resources and Services

More and more, the Library outsources systems and services to third-party vendors. Most of the digital resources that we offer, for example, come from outside suppliers, as does the current [Library Catalog](#) (see the case study below). (The [Classic Catalog](#) is still managed internally.) The Library expects the information service providers with whom we contract to protect the identity of individual users and the information they use. We commonly require, for example that vendors agree not to sell or license information from library users to third parties. Many vendors provide additional personalized services that may require you to identify yourself with your name or a pseudonym. In general, this is done at your discretion; the Library seeks to avoid products that demand personalization.

While the Library seeks to require third parties with which it works to follow accepted library policies regarding privacy and confidentiality, it is not responsible for the privacy practices of these third parties. We encourage users to familiarize themselves with third party privacy policies before using the resources.

Library Surveys/Assessment Projects

Information and data obtained by the Library or its units through surveys (group or individual interviews or other means) in support of assessment of services, collections, facilities, resources, etc., or in support of research related to library and information services, are considered confidential and will not be shared except in aggregations, to protect the privacy of individual participants. When required, surveys are conducted in accordance with the policies of Cornell's [Institutional Review Board for Human Participants](#).

Children Under 13

The Library does not knowingly request, collect, or share personally identifiable information from users under the age of 13.

Contact

If you have questions about the Library's practices regarding privacy and confidentiality, please contact LIBGATEWAY-L@cornell.edu.

Licensed Service Case Study: The Library Catalog

The current [Library Catalog](#) is a good example of the privacy issues that are associated with licensed resources and services. The Library contracts with OCLC Online Computer Library Center, Inc. to provide the [Library Catalog](#). Use of the catalog is governed by the [OCLC WorldCat.org Services Terms and Conditions](#), accessible after one conducts a search in the catalog. The Terms note that "OCLC's collection and use of any personal information submitted via the OCLC WorldCat.org Web site (if any) is governed by OCLC's Privacy Policy, which can be accessed at <http://www.oclc.org/worldcat/policies/privacy/>." While OCLC does collect records of searches in aggregate and does not purge them, according to Cheryl Snowdon, Product Manager for WorldCat Discovery Services at OCLC:

Individual users are not connected to activities performed on the site. Therefore, searches conducted and records viewed cannot be tied back to individual users. IP addresses are collected but they are not tied to any data, including the searches performed.

OCLC also utilizes web beacons and cookies and the services of a third party firm to measure how visitors use our site. They collect the following information on users of the catalog:

- IP address of machine being used
- The domain of that machine
- The host of that machine
- Language set in browser
- Whether cookies are enabled or disabled
- Browser
- Plug-ins being used (e.g. Flash, Acrobat, RealPlayer, etc.)

- What page the user entered the site on (e.g Detailed Record, Search Results), but not the specific record or search conducted
- Referring URL (where the user clicked from to arrive at WorldCat.org/WorldCat Local; includes whether the user clicked from a browser bookmark or whether the page was the home page set in the user's browser)
- Date and time of visits
- Javascript enabled or disabled
- Javascript version
- Java enabled or disabled
- Operating system
- Monitor resolution
- Monitor color depth
- Country
- "Monthly Unique Visitor" (i.e. first visit during the month)

Individual users are not connected to activities performed on the site. Therefore, searches conducted and records viewed cannot be tied back to individual users. OCLC's contract with Omniture also stipulates that data collected from the OCLC web site is the confidential property of OCLC. Omniture therefore cannot disclose or share that information with any third party without OCLC's authorization. Furthermore, it is possible to opt-out of Omniture's cookie tracking at <http://www.omniture.com/privacy/207>.

22 December 2009