NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)

Published on December 10, 2015

Preamble

Support of intellectual freedom and protection of user privacy and user confidentiality have long been integral components of the missions of libraries and related institutions. The management of information resources increasingly involves digital networks that, by their nature, include possibilities for tracking and monitoring of user behavior, whether content or services delivered are physical or digital. As this ecosystem of electronic systems to manage library-supplied resources has grown and expanded beyond the library's internal operations, the larger community of libraries, content-, and software-providers needs to recognize the implications this has on users' privacy. Libraries, publishers, and software-providers have a shared obligation to foster a digital environment that respects library users' privacy as they search, discover, and use those resources and services.

Certain personal data are often required in order for digital systems to deliver information, particularly subscribed content. Additionally, user activity data can provide useful insights on how to improve collections and services. However, the gathering, storage, and use of these data must respect the trust users place in libraries and their partners. There are ways to address these operational needs while also respecting the user's rights and expectations of privacy.

Information management practices, security protocols, and legal frameworks evolve over time, and that evolution has implications for user privacy. It is therefore incumbent on all participants in the information ecosystem to strive toward continuous improvement of their activities and policies to ensure the most appropriate level of protection for users' personal data.

The principles outlined in this document are a starting point. Additional community consensus work will be necessary to make some of these principles implementable by the spectrum of providers that supports library services. We encourage all those involved in provision of library-user services to contribute to future work related to the themes covered below.

Through the following principles, we strive to encourage consensus around practices and procedures that protect the digital privacy of the library user.

1. Shared Privacy Responsibilities

As expressed in these principles, the ALA Code of Ethics, and the IFLA Code of Ethics, libraries and librarians have an ethical obligation—and in some cases a legal obligation—to preserve users' privacy and to prevent any unauthorized collection, use, or disclosure of library users' data. Publishers and software-providers, which operate through and for the library and its users, share in this ongoing ethical responsibility. Anyone with access to library data and activity should accept responsibility for safeguarding user privacy and data security and should have training in related standards and best practices.

2. Transparency and Facilitating Privacy Awareness

Library users need to be able to determine the extent of privacy protections provided and the boundaries of those protections as they use library resources. Libraries, content-, and software-providers shall make readily available to users specific, non-technical statements that describe each stakeholder's policies and practices relating to the management of personally identifiable information. These policies should also inform library users how they can protect the privacy of their data themselves. Such statements shall identify what data are collected, why data is collected, who has access to the data, how the data are stored and secured, when that data might be disclosed and to whom, and what the organization's data retention and/or deletion policies are.

Library users can best take advantage of the privacy protections afforded by libraries if they understand the extent to which their privacy is and/or is not protected. Means of communicating privacy choices to users include outreach, inclusion of library-user communication methods in systems design, and user education. All parties involved in providing services should effectively communicate those choices to users. Systems should be designed in a way that facilitate understanding of policies through the use of simplified management of options.

3. Security

The most current security best practices should be used as the baseline to protect data. These should include encryption of personal data while they are at-rest and in-motion; prompt updates of systems and software to address vulnerabilities; systems,

procedures, and policies for access control of sensitive data; a procedure for security training for those with access to data; and documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.

Unauthorized access to user data should be remedied in a timely manner in order to minimize exposure of such data and affected parties should be informed as soon as is practicable in compliance with applicable laws. Libraries, content-, and software-providers should comply with applicable statutory or regulatory requirements and published security standards intended to promote the privacy and security of user data.

4. Data Collection and Use

The potential benefit to the user, the library, content-, or software-provider derived from the collection and use of users' personal data must be balanced against the impact of that collection and use on users and their right to privacy. Collection and use of users' personal data should be for the purposes of supporting user services, research to improve those services, or for the internal operations of the library, content-, or software-provider for which the data were gathered. The effective management and delivery of library services may require the library user to opt into the provision of personal data in order to access a library resource or receive library services. Users' personal data should only be used for purposes disclosed to them and to which they consent.

Certain types of personal data (e.g., regarding race, gender, socioeconomic class, ability, etc.) are perceived to be more sensitive, and if they are to be held or used by a library, content-, or software-provider, should require higher levels of scrutiny and justification. In addition, such data require extra protection once they are collected.

5. Anonymization

That portion of library user data that includes personally identifiable information should be retained in that form only as long as absolutely necessary for operational purposes. After operational needs expire, if data are to be retained for research purposes or in support of administrative objectives, personally identifiable information should be masked through anonymization processes unless users have consented to retention of personally identifiable information. Anonymization should be used as part of a broad set of information privacy controls that include: data minimization; statistical disclosure limitation methods, such as controlled aggregation; data-use agreements; and auditing.

Anonymization may not completely eliminate the risk of re-identification. Therefore even anonymized raw data should be treated with the precautions detailed in the Security principle (item 3 above), in proportion to the potential risk of re-identification.

6. Options and Informed Consent

Each library user's needs and expectations of privacy are different and may be contingent on circumstances. When personal data are not required to provide services as described in "Data Collection and Use", libraries and content- and software-providers should offer library users options as to how much personal information is collected from them and how it may be used. The default approach/setting should be that users are opted out of library services until they explicitly choose to opt in. In cases where a user opts in to a specific service, they should have the choice to opt out at a later date, in particular when privacy policies change, and at that time have the option to delete data as outlined in "Access to One's Own User Data" (item 10 below).

7. Sharing Data with Others

Libraries, content-, and software-providers sometimes need to share some data to provide content or library services, or undertake administrative functions. However, these parties must carefully consider the impact on the user's privacy before sharing data or information about their activity with third parties. Such considerations should include: the library user's consent; the user's privacy interests; any legal prohibitions or requirements; the policies of that third party and their adherence to these principles; and the risks and benefits to the user and institution.

User activity data to be shared should be anonymized and aggregated to a level that minimizes privacy risks to individual users, unless the user has opted-in to a service. In particular, possible exposure of the resource-use habits of individual users should be protected in conformance with the "Anonymization" principle (item 5 above).

8. Notification of Privacy Policies and Practices

T*o support the policies outlined in the "Transparency" section (item 2 above), privacy policies should be made easily available and understandable to users. These policies might change over time, so providers of library services should publish notice of any significant changes to their privacy policies, and there should be an effort to directly notify impacted users of any changes to the library's or vendor's privacy policies. Changes to policies should not be applied retroactively to user data without users' consent except as required by law.*

9. Supporting Anonymous Use

Libraries and content- and software-providers must recognize the right of library users to be anonymous, should they so choose, and users should be provided appropriate affordances. Not all service capabilities may be available while a user remains anonymous, but reasonable accommodations to provide basic services should be made. When the collection and retention of a user's personal data are required in order to access library resources or deliver library services, the library user should be informed that anonymous service is not possible.

10. Access to One's Own User Data

Users should have the right to access their own personal information or activity data. Users should be provided, in so far as is feasible, access to these data for review, so that users may request correction or deletion. Organizations holding these data should make their best effort to provide it. Some records may not be able to be deleted if they are required by the library, content-, or software-provider for internal operations or business purposes as described in "Data Collection and Use" (item 4 above). As an optional service, providers might make these data securely exportable in common file formats.

11. Continuous Improvement

Libraries, content-, and software-providers should continuously assess and strive to improve user privacy as threats, technology, legal frameworks, business practices and user expectations of privacy evolve.

12. Accountability

Libraries, content-, and software-providers should establish a culture of accountability in which data collection, security, use, sharing, and disposal practices and policies are reviewed and reported on a periodic basis. Accountability practices will evolve over time, but they should include, where appropriate, periodic reviews or audits of computer systems, security practices, policies, and procedures, preferably by independent third parties. The conclusions of reviews or audits should be available to libraries on request.

Glossary

***Anonymization**: The process of transforming or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.*
***ALA:** American Library Association*
***Content provider:** Any entity that provides content to library users under an agreement with the library. An entity can simultaneously be both a content- and a software- (or systems-) provider.*
***Data at-rest, data in-use, and data in-motion**: Terms describing the status of personally identifiable information or personal activity data housed within library, content- or software-provider infrastructure. Data at-rest describes data while it is stored within systems. Data in-use means data that is being processed or used to provide a service. Data in-motion is data that is being transferred for storage or processing.*
***Informed Consent:** An individual's ability, based on access to information in privacy policies, to determine whether or how their personal information may be used or disclosed by the entity that collected the information.*
***IFLA:** International Federation of Library Associations and Institutions.*
***Internal operations:** Business or administrative processes or activities undertaken to provide, maintain, improve, or support core objectives of the organization.*
***Library services:** The activities a library either directly provides, enables, or hosts, or contracts with an outside organization to provide, enable, or host, that support the mission of the library and assist the patron or user of library resources.*
***Library user:** Anyone who avails of library services, materials, or systems. This includes patrons, library staff, volunteers, and any other community member accessing library resources or services.*
***Software provider**: Any entity that provides digital systems and/or services that facilitate the management, discovery, delivery, use, or preservation of library owned or licensed resources. An entity can simultaneously be both a library, a content- and a software- (or systems-) provider.*
***Personal activity data:** Data that is generated by a library user's activity in a library context that can be traced to that individual. Examples include circulation records, search, browsing and download history, social media interactions, online communications history (e.g., email, SMS, etc.), library activity logs, reading behavior data, authentication logs, and computer-use data.*
***Personally identifiable information (PII):** Data that can be used—on their own or in combination with other data—to identify, contact, or locate a single person, or to identify that individual in context. Also called personal information.*

Privacy: *As defined by National Research Council and the Social Science Research Council; "Informational privacy encompasses an individual's freedom from excessive intrusion in the quest for information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions, and attitudes will be shared with or withheld from others." (Report of the National Academy of Science 1993 Panel Report Private Lives and Public Policies, p. 22) There are many other definitions of privacy in an information environment and there is no consensus about all the elements that privacy covers.*

Privacy policies: *The public description of the processes and practices that outline how an organization gathers, uses, discloses, and manages personally identifiable information and personal activity data.*

Third-parties: *Entities that are neither libraries, content providers, nor systems providers and who are not directly tied to the operational provision of services to the library user.*

Related Reading

ALA Code of Ethics

http://www.ala.org/advocacy/proethics/codeofethics/codeethics

IFLA Code of Ethics

http://www.ifla.org/news/ifla-code-of-ethics-for-librarians-and-other-information-workers-full-version

---

The creation of these principles was funded by a generous grant from the Andrew W. Mellon Foundation.