DRAFT RECOMMENDATIONS FOR A PRIVACY POLICY COMPONENT FOR THE NSDL MOU

Jim Burger, Mick Khoo, Eileen McIlvain

April 24, 2006

Summary

We recommend that:

1 That the existing MoU wording, section 3.3.3, be replaced with the wording proposed in this document
2 That the Appendix included in this document be added to the end of the new MoU

1 Replacement of existing MoU wording

Existing MoU Wording

3.3.3 Post privacy policy on portal site
- Help define minimum elements required for consistency across all sites
- Meet COPPA guidelines, where required

Proposed MoU Wording

3.3.3 Pathways projects should provide provide privacy policies that are easy to read, and easily accessible. Appendix X of this MoU contains a set of minimum elements, and minimum recommended wordings, that each Pathway is expected to adopt and/or incorporate into their own individual privacy policies.

2 New Appendix for the MoU

Appendix

NSDL Privacy Policies

A privacy policy is a vital trust component of any web site. A comprehensive, clear, easy to find and easy to read privacy policy, can go a long way towards building up a good relationship between a web site and its users. Conversely, privacy policies that are hard to find, hard to read, or otherwise hard to use, can damage the trust that a user has in a web site.

A privacy policy is particularly important in the case NSDL, which offers a range of customizable services, and offers these services to children and to young people in educational settings traditionally associated with trust. NSDL's ability to offer these customizable services increasingly depends on identifying repeat visitors to the library, but the implementation of visitor identification processes, such as Single Sign On, raises a number of potential privacy concerns with regard to the collection of user information by NSDL, particularly with regard to cases where information is collected from children aged under 13.

NSDL does not at present possess a program-wide set of standardized privacy policy practices that addresses these issues. Currently, privacy policies are developed and implemented on an individual project basis. In order to assure the quality and trust of the NSDL program as a whole, and also to locate accountability for this quality and trust in an easily identifiable organization, it is desirable for NSDL recommend a 'bare-bones' set of privacy policy categories, that should be adopted by signatories to the Memorandum of Understanding.

This appendix outlines therefore a minimal, standardized set of privacy policy categories and associated best practices, for NSDL Pathways projects' privacy policies. These clauses may be used verbatim or may be adapted to suit the needs of individual projects. However,

while Pathways projects remain free to develop their own privacy policies, they are also expected to address all of these minimal recommendations.

The privacy policy categories discussed in this appendix are:

- Privacy policy usability
- Introduction to and explanation of privacy policy
- Policy scope
- Organizational contact information
- Web metrics
- User registration/Personal accounts
- HTTP Cookies
- Child Online Privacy Protection Act (COPPA) requirements
- Compliance with court orders

Each of these categories will be discussed in a separate section, consisting of a short *background discussion* of the privacy issues involved, followed by draft *recommendations* for a relevant privacy policy clause that addresses these issues.

These best practices are not intended as replacements for existing NSDL privacy policies under discussion by the NSDL Policy Committee; these latter discussions apply only to nsdl.org, and not to the individual Pathways projects.

Further Information

For further information, and for examples of existing NSDL Pathway privacy policies, please see:

URL OF WEB SITE TO BE CONSTRUCTED GOES HERE. (HAVE THIS ON EV – SO PEOPLE CAN POST QUESTIONS? WOULD NEED AN ALERT SERVICE FOR THE QUESTION ANSWERER).

Contact Information

If you have any questions about these guidelines or their implementation, please contact:

CONTACT INFO HERE

Privacy Policy Usability

Background

A privacy policy is a vital trust component of any web site. A comprehensive, clear, easy to find and easy to read privacy policy can go a long way towards building up a good relationship between a web site and its users. Conversely, privacy policies which are hard to find, hard to read, or otherwise hard to use, can damage the trust that a user has in a web site.

A privacy policy is therefore not useful unless it is easily accessible. Accessibility factors include: whether or not the policy is easy to find on a project web site, and whether or not it is written in plain English, or has a plain English summary.

Recommended actions

[Note: In this case, these recommendations are for privacy policy best practices, rather than for specific privacy policy wordings. These recommendations will appear in the MoU, and not in the privacy policies themselves.]

General Requirements

Accessibility

- The privacy policy should be accessible from all the pages on a web site

The link to the privacy policy page

- The link to the privacy policy should be prominently displayed
- The link should be in black font at least the same size as the rest of the page content
- The link should be at the top of the page (i.e. the user should not have to scroll down to access the link)
- If an image is used as a link to the privacy policy, a suitable alt tag must be supplied

Page formatting

- The privacy policy page should be in black font at least the same size as the rest of the web site content. The page should be easily printable.
- The privacy policy should be written in plain language. Where, for legal reasons, a web site is obliged to post a long, legally correct privacy policy, a prominent link to a short, easy to read summary should be provided.

Content

- The privacy policy page should not include non-privacy related content such as ‘terms of use,’ ‘users’ responsibilities,’ etc.

Screenreaders

- The privacy policy page should be accessible to screen readers.

Introduction to and explanation of privacy policy

Background

The function and nature of privacy policies is not always immediately obvious to the user. Each privacy policy should therefore begin with a brief introduction outlining the purpose of the policy.

Recommended wording

Introduction

This project collects different types of data from web site visitors to this site, including yourself. These data may include your IP address, the date and time of your visit, the type of operating system and web browser that you use, and so on. These data are used for instance to analyze web site visits, and to support tools to enhance user experience.

Different data are collected and stored in different ways, which have different implications for your privacy. NSDL supports a standardized set of privacy policies and practices, which balance the privacy needs of its users with the library's ability to provide users high quality and customizable access to its resources. This privacy policy outlines the different forms of data being collected by this project, and the ways in which it is being stored and safeguarded.

If you have any questions about this project's privacy practices, please contact the person named below.

Contact information

Background

Each privacy policy should prominently display a contact for information about the privacy policy.

Recommended Wording:

Contact information
If you have any questions about this project's privacy policies, please contact:
NAME AND JOB DESCRIPTION
MAILING ADDRESS
TELEPHONE NUMBER
FAX NUMBER
E-MAIL

Policy Scope

Background

The NSDL program supports distributed, federated search across a large number of partner collections. Individual NSDL collections may have their own sets of privacy practices and policies. The federated nature of NSDL may not be obvious to all users, who may be under the impression that the NSDL 'brand' designates a single institution.

The privacy policies of individual sites should therefore define, in a prominent position, the site(s) that they apply to, and they should also warn users that upon leaving these site(s), the privacy policy in question will no longer apply.

Recommended wording

Scope of this policy

This policy applies only to the web site for 'NAME OF PROJECT' (URL OF PROJECT). Please note that if you leave this web site for another web site, including the web site of another NSDL project, this privacy policy will no longer apply.

Web Metrics

Background

NSDL Pathways use a range of different web metrics to track their site usage. The idea that a web site is collecting data on them may cause worry to some users, and it is good practice therefore to be open about the different types of web metrics being used, and their individual privacy implications. This is particularly true with respect to the use of Omniture, as Omniture collects web metrics through javascript embedded in each page, as well as a longer piece of javascript kept on each server. In terms of developing and preserving trust between users and NSDL Pathways, it is advisable to have a full description of this technology, and its privacy implications, in the privacy policy.

Recommended Wording:

Web Metrics

This web site uses web metrics to record the details of your visit. This involves collecting data such as the pages you have viewed, the browser you have used, and so on. Web metrics data can range from the anonymous (e.g. time/date of visit) to the identifiable (e.g. IP address). These data provide useful statistics for project managers and project funders, and support the improvement of web site design. These data are always anonymous, and almost always aggregated.

This web site collects two different forms of web metrics: first-party (transaction log) metrics, and third-party metrics.

In the case of first-party web metrics, these are collected by this project on our own project server. [NEED FIRST-PARTY WEB METRICS PRIVACY CLAUSE HERE]

In the case of third-party web metrics, NSDL has contracted a third party, Omniture Corporation (http://www.omniture.com/), to implement standardized webmetrics for a selected number of NSDL partner projects, including this project. NSDL uses third-party web metrics in order to provide standardized baseline web metrics across a number of NSDL projects. These webmetrics are implemented with a combination of session (non-persistent) cookies, and a short piece of javascript that is embedded in each of the this web site's pages, and which is triggered every time that you load a page. This technology allows Omniture to track user interactions with nsdl.org site useage without having direct access to nsdl.org servers.

All data collected by Omniture belong to NSDL Core Integration, and not to Omniture. Access to Omniture webmetrics data is therefore only available to NSDL Core Integration, and is password protected. These data will only be made public (for instance in reports) in anonymous and aggregated form.

User registration and Personal Accounts

Background

User registrations require users to provide an account name and password in order to view a site. Once logged in, each user can then be tracked through that site. Note that users can be tracked through as combination of cookies, account names and passwords, and that more personally identifiable data (such as e-mail addresses and IP addresses) need not be used. In addition to allowing basic access to a site, user registration can also provide users with additional site functionality, such as 'premium' content, newsletters, etc. A proposed NSDL user registration tool, known as 'Single Sign-on,' will allow a user to create an anonymous online identity that permits seamless transitions between various NSDL sites that require individual user registrations.

A 'user registration' privacy clause should state what types of registration data are collected, how these data are being stored, and how they are kept private. In addition, a boilerplate user registration clause specifically describing and tailored to the characteristics of Single Sign-on should be appended by individual projects to their own privacy policies.

Personal accounts are augmented user registration accounts that may offer a range of additional functionalities, such as e-mail alerts and newsletters, personal work areas and folders, access to restricted content such as high-bandwidth audio-visual content, and use of online chat and web logs. To support this increased functionality users will voluntarily have to submit additional personal data, such as e-mail addresses and home page URLs, to the web site in question. A 'personal account' privacy clause should therefore state that, in cases where personal accounts are created, what types of personal data are being collected, how these data are being stored, how personal data will be kept private, and in general spell out the privacy implications of applying for the personal account in question.

Recommended wording

Registration

Some NSDL-funded websites offer users resources that can be customized or that invite participation to a greater extent then simply browsing free-access pages would allow. Those sites invite users to register – for free – for individual user accounts. Registering for such accounts requires voluntary online submission of pertinent user information, or attributes.

When a user registers for an account with NSDL or NSDL funded resources, the following information may be collected:

1. Name (First and Last OR Username)
2. Email Address
3. Position/Job Title/Subject Expertise
4. Personal password

NSDL will use this information for the following purposes:

1. Allowing access to appropriate content
2. Personalizing content based on area of interest/need
3. Web Metrics
4. Issuing updates, invitations, newsletters, etc.
5. Confirming personal acccounts

In the event that collected information will be used for purposes other that those described above, users will be notified of such changes and will be given the option to opt out of those furtherances.

Personal Accounts
Users should be aware that any information about themselves that they post in a publicly viewable place, such as customize homepages, discussion forums, etc., may be seen by other users as well as by site administrators. This Privacy Policy covers information communicated between the NSDL and the user for activities such as account registration and maintenance, but when the user communicates their information in a publicly viewable web space, the degree of privacy or anonymity covering that information is entirely up to the individual user. Because of this, NSDL recommends that users under the age of thirteen not participate in publicly accessed forums or services.

HTTP Cookies

Background

HTTP Cookies are small text files that a website uploads to a users computer in order to provide the users computer with enough information that it remembers the user's previous visit(s). This allows the user to access certain features of the website more efficiently than they would if it was a first visit or if a computer is set to not accept cookies.

While cookies in general are innocuous, they have also raised controversy as some people feel that there are similarities between having a cookie on a computer and having a surveillance device in their homes. This is however a misunderstanding of the underlying technology of cookies. While they do convey information about a user, this is solely information about a user's computer and browser session (IP address, navigation, etc.), and this information is collected for the purposes of authentication, user tracking, and maintaining user preferences.

It is important to explain the use of cookies to your users in a clear and simple way. Some good information about cookies can be found on Wikipedia at http://en.wikipedia.org/wiki/HTTP_cookie

Recommended wording

Cookies

HTTP Cookies are small text files that a website uploads to a users computer in order to provide the users computer with enough information that it remembers the user's previous visit(s). This allows the user to access certain features of the website more efficiently than they would if it was a first visit or if a computer is set to not accept cookies.

While cookies in general are innocuous, they have also raised controversy as some people feel that there are similarities between having a cookie on a computer and having a surveillance device in their homes. This is however a misunderstanding of the underlying technology of cookies. While they do convey information about a user, this is solely information about a user's computer and browser session (IP address, navigation, etc.), and this information is collected for the purposes of authentication, user tracking, and maintaining user preferences.

There are two types of HTTP cookies

1. Session cookies are cookies that reside on the user's computer only during the time when the user is online at the cookie providing website. These allow the online system to respond more quickly and personally during the user's session than it would be able to without having the preloaded information that the cookie enables.
2. Persistent cookies are cookies that remain on a users computer after closing the browser session during which the cookie was downloaded on the local computer. Persistent cookies allow fast access during subsequent visits to the website.

Any computer can be configured to accept all cookies, accept some cookies, or accept no cookies. Accepting no cookies can often prevent full use of a particular website which might require the use of cookies. Additionally, cookies can be set to expire, so that after a certain amount of time elapses between uses the cookies are simply deleted from the user's computer.

Some good information about cookies can be found on Wikipedia at http://en.wikipedia.org/wiki/HTTP_cookie

The Children's Online Privacy Protection Act (COPPA)

Background

All NSDL web sites must operate in compliance with the Children's Online Privacy Protection Act (2000). The principle concern here concerns the collection of personal information (for instance in the form of user registration or personal accounts – see above) from children under 13 years of age. Information classified as personal includes "individually identifiable information about a child that is collected online, such as full name, home address, e-mail address, telephone number or any other information that would allow someone to identify or contact the child." The Act and Rule also cover other types of information – for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms – when they are tied to individually identifiable information."

The Child Online Privacy Protection Act (COPPA) is enforced by the Federal Trade Commission and outlines specific measure a website must take to protect the privacy of children (minors under the age of 13).

NSDL believes that even the types of websites that are not specified in the Act should make every reasonable effort to adhere to the FTC's rules, which are reasonable and for the most part simple to implement. The basic function of the rules is to

- List starts here
- List continues here
- List continues here
- List ends here

COPPA works by using a sliding scale approach. That is, the more commercial a website is and the more use it makes of personal information – especially in sharing it with others – the greater the efforts that need to be made in protecting privacy and adhering to the rules. In general, NSDL websites, being educational (non-commercial) in nature and not sharing personally identifying information with third parties for marketing purposes, can adhere to the lower end of the sliding scale.

NSDL suggests that all NSDL-funded projects follow these measures to ensure COPPA compliance:

- List starts here
- List continues here
- List continues here
- List ends here

Recommended wording

Child Online Privacy and Protection Act

The Child Online Privacy Protection Act (COPPA) is enforced by the Federal Trade Commission and outlines specific measure a website must take to protect the privacy of children (minors under the age of 13). NSDL believes that even the types of websites that are not specified in the Act should make every reasonable effort to adhere to the FTC's rules, which are reasonable and for the most part simple to implement.

The basic function of the rules is to require website operators to:

- Incorporate a detailed privacy policy that describes the information collected from its users.
- Acquire verifiable parental consent prior to collection of personal information from a child under the age of 13.
- Disclose to parents any information collected on their children by the website operator.
- Grant the parental right to revoke consent and have information deleted.
- Limit collection of personal information when a child participates in online services.

- Protect the confidentiality, security, and integrity of any personal information that is collected online from children.

COPPA works by using a sliding scale approach. That is, the more commercial a website is and the more use it makes of personal information – especially in sharing it with others – the greater the efforts that need to be made in protecting privacy and adhering to the rules. In general, NSDL websites, being educational (non-commercial) in nature and not sharing personally identifying information with third parties for marketing purposes adhere to the lower end of the sliding scale.

NSDL-funded projects take the following measures to ensure COPPA compliance:

· [these need clarity and greater specificity]
· Confirmation of registrants age
· Collection of parental and/or guardian contact info
· Parental notification
· Anonymity

Compliance with court orders

Background

Each project should detail how it will respond to court requests, orders or subpoenas for data stored on its servers.

Recommended wording

Compliance with court orders

NSDL will not voluntarily share user information with parties outside of the project's scope. In the event of a subpoena or court order for the release of such information to local, state, or federal courts, NSDL will comply with the jurisdictional law regarding such a transmission of information and will supply only that information which it is legally compelled to hand over. Every reasonable attempt will be made to preserve the anonymity and/or privacy of individuals identifies in whatever data is subpoenaed. NSDL will also make reasonable and legal effort to inform users about the transmission of such subpoenaed data.