A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards?

Trina J. Magi

Librarians have a long history of protecting user privacy, but they have done seemingly little to understand or influence the privacy policies of library resource vendors that increasingly collect user information through Web 2.0-style personalization features. After citing evidence that college students value privacy, this study used content analysis to determine the degree to which the privacy policies of 27 major vendors meet standards articulated by the library profession and information technology industry. While most vendors have privacy policies, the policy provisions fall short on many library profession standards and show little support for the library Code of Ethics.

Librarians have a long history of protecting the confidentiality of library users, believing that free people have the right to read freely without being monitored, judged, ostracized, or surveilled. They have expressed support for this right in the American Library Association (ALA) *Code of Ethics* and other documents, adopted confidentiality policies for their libraries, and publicly defended reader privacy against threats by the government. There is evidence that the public supports and appreciates this work.

Research shows that in the highly interactive Web 2.0 environment, with its emphasis on information *sharing* in addition to browsing, youth and college students still value privacy, although they sometimes behave in ways that seem at odds with that value. The Web 2.0 environment, however, poses new challenges for librarians in their commitment to protect user privacy, as vendors of online library databases incorporate personalization features into their search-and-retrieval interfaces, thereby collecting personally identifiable user information not subject to library oversight.

Surprisingly, the library literature reveals no in-depth examination of the privacy policies of vendors of library online resources. Do vendors collect user information? If so, do they handle that information in accordance with privacy standards articulated by the library profession and the information technology industry? Primarily using content analysis, this study sought to answer these important questions. If librarians continue to assure users that their library searches and research interests are confidential but know nothing about the privacy policies of the vendors who provide the databases offered by the library, librarians risk betraying their users' trust.

Trina J. Magi is Library Associate Professor in Bailey/Howe Library at the University of Vermont; e-mail: trina.magi@uvm.edu. *Acknowledgment: The author gratefully acknowledges the assistance and support of Douglas Dunbebin, Alan Howard, Milton Crouch, and Martin Garnar.*

Literature Review

Librarians and Privacy

For many decades, librarians have believed that protecting user privacy is a professional responsibility. Each version of the ALA *Code of Ethics*, including the original published in 1939, has contained language upholding that principle.[1] This position reflects the belief that libraries and librarians should foster intellectual freedom by giving users the ability to read, view materials, ask questions, and conduct research without having to worry about surveillance, judgment, or ostracism. A person has full access to information only when there is no fear of recrimination.[2] This ability to freely access information is important in a democracy where people are to be their own governors, and it is integral to the freedom of speech promised by the First Amendment.[3]

Recently, librarians received attention and praise for raising concerns about the USA PATRIOT Act, a federal law enacted in 2001 and reauthorized in 2006. The USA PATRIOT Act gave law enforcement greater access to library and other business records.[4] This was not the first time librarians had resisted law enforcement threats to user privacy. In 1970–1971, librarians criticized the Alcohol, Tobacco, and Firearms Unit of the Internal Revenue Service for seeking library records in connection with investigations into planting bombs.[5] In the late 1980s, librarians resisted the FBI's "library awareness program," in which FBI agents made visits to research libraries and asked library personnel to report on the reading and research habits of people, especially "foreigners."[6]

Public Attitudes about Privacy

Librarians have won public support for their commitment to privacy. Currently all states plus the District of Columbia provide some measure of confidentiality protection for library users either in state law or through opinion of the state attorney general,[7] and there is other evidence that people care about privacy. Best, Krueger, and Ladewig reviewed trends in public opinion poll results concerning privacy from 1990 through 2006 and generally found that concern about threats to privacy has been growing in recent years.[8] A six-country survey conducted by Harris Interactive for OCLC investigated the values and social-networking habits of library users and found that nearly three quarters of respondents indicated that it is extremely or very important to be able to control who can use and view their personal information on the Internet. About half feel it is extremely or very important that the library keep information about the books they read and other library activities private.[9] McCullagh's survey of 1,258 bloggers worldwide found that bloggers value privacy, and only 2.8 percent were not at all concerned with protecting personal information.[10]

Further evidence that people care about privacy and control over personal information can be found in the outrage that followed Facebook's launch of two features that automatically notified people about others' activities online, including products purchased. More than 700,000 users of the social networking site signed a petition opposing "News Feed," a feature introduced in September 2006,[11] and about 50,000 users joined a group opposing "Beacon," introduced in November 2007.[12] In 2009, Facebook again faced a firestorm of criticism after it made a change to its terms of service that many users interpreted to mean Facebook would own user content, even if a user deleted his or her profile. A member group called "People against the new Terms of Service" (TOS) drew more than 86,000 members, and a coalition of privacy advocates including the Electronic Privacy Information Center threatened to file a formal complaint with the Federal Trade Commission.[13]

Privacy Attitudes and Practices among Teens and College Students

While it is true that many young people share intimate details of their lives on the Web,[14] it is also true that many young people care about privacy. Johns and Law-

son surveyed 444 undergraduate students about their knowledge of the personal information their library may store and their opinions about reasons for collecting and using that information.[15] Most students (85%) said online privacy was important or very important to them, and another 10 percent said it was somewhat important. The survey also found that large majorities of students agreed that a university or library 1) should obtain private information only with students' consent (92%); 2) should collect student information only for clearly defined purposes (86%); 3) should never disseminate students' personal information to outside agencies (91%); and 4) should assign appropriate life spans for the retention of student information (74%). A large majority (77%) of students also felt it was *not* justifiable to develop student profiles for the purpose of improving library collections and services, and 78 percent of students agreed or strongly agreed the library should inform students about the USA PATRIOT Act.

Other studies have examined the attitudes and behaviors of young people online. Youn found that, while using the Web, teenagers engage in privacy-protecting strategies such as falsifying or providing incomplete information, or using alternative Web sites that don't request personal information.[16] Moscardelli and Divine's survey of high school students showed support for the proposition that "increasing adolescents' concern for their online privacy leads to greater use of privacy-protecting behaviors."[17] In a 2006 survey of 935 American teens, Pew Internet & American Life Project found that although teens engage in risky behavior online, for many, "privacy and disclosure choices are made as they create and maintain social networking profiles" and "most teenagers are taking steps to protect themselves online from the most obvious areas of risk."[18] Steps include not posting a last name or cell phone number, withholding specific location information, posting false information, and restricting access to online profiles.

Despite people's concern that their right and ability to control personal information may be violated, they often give personal information freely or fail to take steps to protect their privacy. Numerous researchers have compared people's attitudes and intentions about privacy with their actual information disclosure behaviors and identified this "privacy paradox."[19] The privacy paradox is also found among young people. Barnes' survey of college students found strong disagreement with the statement, "Everybody should know everything about everyone else," yet she notes that young people freely give up personal information. She suggests this is because "the private versus public boundaries of social media spaces are unclear. On the Internet, the illusion of privacy creates boundary problems."[20] Students may not understand that parents, future employers, and university officials can read journal entries intended for their online friends.

Web 2.0, Library Vendors and Privacy

Many librarians have gone to great lengths to assure the public that they will protect the confidentiality of library users' reading and research interests. For example, librarians have worked to protect the confidentiality of their users when they search the online catalog, check out materials, or ask reference questions. However, they have not typically addressed a growing potential privacy threat posed by vendors of Web-based information resources.

The Web 2.0 environment, with its emphasis on interactive information *sharing* in addition to browsing, poses new challenges in the effort to protect user privacy. For a long time, users have been able to send database search results to themselves or others by supplying e-mail addresses. Now many vendors of online products have begun to incorporate personalization features into their search-and-retrieval interfaces, inviting users to create personal profiles and online repositories where they can record their research interests, search strategies, and favorite articles (for instance, CQ Press's

"Your Profile"; EBSCO's "MyEBSCOhost"; Elsevier's "My Settings").

Corrado recognized the privacy threat posed by information being held on vendor servers, observing, "Libraries have a significant investment in databases that are housed by commercial vendors outside the library. These commercial vendors may not have the same privacy concerns and policies as the library, however very few libraries warn patrons about this when they link to remote sources on their Web site."[21] Luther also acknowledges that online publishers who offer personalized or customized services must retain user-specific information, and she says protecting users' privacy rights should extend into the electronic environment. It is the obligation of publishers to develop policies for protecting user information, she says.[22] Woodward advises librarians to check the privacy policies of subscription database vendors and publishers that may be keeping data about library users and to "exert their power of the purse when dealing with vendors."[23] Litwin also acknowledges the tension between Web 2.0 applications and librarians' core value of privacy, and calls for more discussion of the issue.[24]

In spite of the growing threat, the literature reveals little activity on the part of librarians to either understand or influence the user confidentiality practices of the vendors with whom they contract. Sturges, Davies, Dearnley, Iliffe, Oppenheim, and Hardy interviewed representatives of 14 companies that supply library management software systems and reported that, according to respondents, "there was no evidence in the responses that libraries paid any special attention to privacy in the negotiations over systems."[25] In 2002 the International Coalition of Library Consortia (ICOLC) issued "Privacy Guidelines for Electronic Resource Vendors" in an attempt to encourage vendors to adopt privacy policies that conform to the ALA *Code of Ethics*.[26] There was no long-term follow-up or formal examination of vendor compliance with the guidelines, however, according to former ICOLC member George Rickerson (as reported in a telephone conversation with the author on October 10, 2008). The most recently published *Survey of Library Database Licensing Practices*—more than 100 pages long—reported practices and trends in more than a dozen aspects of database licensing but made no mention of the issue of privacy of user data.[27]

Research Questions

Because so little has been published in this area, it was not possible to formulate hypotheses concerning library vendors' privacy policies. Instead, the project posed and answered several research questions:

1. Do vendors have written privacy policies?
2. Do vendors make these policies readily available to users?
3. To what degree do the existing policies meet privacy standards expressed by the information technology industry?
4. To what degree do the existing policies meet privacy standards expressed by the library profession?

Privacy Standards

To answer research questions 3 and 4, it was necessary to first gather a list of privacy standards. In response to public concern about privacy and in an effort to promote self-regulation, government and business organizations have published standards for handling data and informing consumers. Library organizations have also published recommendations and guidelines about privacy. These standards, described below, provide a rational basis against which the policies of library vendors can be measured.

Information Technology Industry Standards

In 1980 the Organisation for Economic Co-Operation and Development (OECD), of which the United States is a member, adopted the "Recommendation of the Council Concerning Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data." These guidelines were intended to provide a foundation for

national privacy legislation, uphold human rights, and prevent interruptions in international flows of data.[28] The U.S. Federal Trade Commission (FTC) cites these and other guidelines in a document titled "Fair Information Practice Principles," which identifies and describes five core principles of privacy protection: 1) Notice/Awareness, 2) Choice/Consent, 3) Access/Participation, 4) Integrity/Security, and 5) Enforcement/Redress.[29] According to TRUSTe, a private organization that uses these principles to help companies develop and implement policies and resolve disputes, "the Federal Trade Commission's Fair Information Practices are the closest thing the industry has to an online standard for privacy practices. The Fair Information Practices are based on the principles of full disclosure that underlie an enlightened democracy."[30] Table 1 presents a summary of the principles, prepared by TRUSTe.

Library Profession Standards

Since the 1930s, the ALA *Code of Ethics* has advocated the protection of user privacy. Based on the *Code of Ethics*, ALA also has generated numerous documents that articulate standards regarding user data collection, management, and disclosure. The following statements have been adopted by ALA Council, the association's official governing body: "Privacy: An Interpretation of the Library Bill of Rights,"[31] "Policy on Confidentiality of Library Records,"[32] "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users,"[33] and "Resolution on the Retention of Library Usage Records."[34] Together, these official statements provide a set of best practices for librarians to follow in handling data about their users.

TABLE 1
U. S. Federal Trade Commission Fair Information Practice Principles (as summarized by TRUSTe)

Notice/Awareness: Web sites should provide full disclosure of what personal information is collected and how it is used.
Choice/Consent: Consumers at a Web site should be given choice about how their personal information is used.
Access/Participation: Once consumers have disclosed personal information, they should have access to it.
Integrity/Security: Personal information disclosed to Web sites should be secured to ensure the information stays private.
Enforcement/Redress: Consumers should have a way to resolve problems that may arise regarding sites' use and disclosure of their personal information.

There is considerable agreement among the ALA and FTC principles. For example, both stress the importance of having a policy and making it available (notice/awareness) and keeping data secure (integrity/security). However, the ALA principles go beyond transparency and an "informed consumer" and call for librarians to refrain from collecting data when possible, and to actively prevent its disclosure to any person or group except in response to a court order based on good cause.

Although the ALA recommendations were designed to apply to libraries, the 2004 "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users" says confidentiality protection should extend to database search records. The 2006 "Resolution on the Retention of Library Usage Records" clearly recognizes that, in a networked world, library user data often flow outside the confines of the library, and users deserve to be protected when that happens. The resolution urges all libraries to "ensure that the library work with its organization's information technology unit to ensure that library usage records processed or held by the IT unit are treated in accordance with library records policies," and "assure that vendor agreements guarantee library control of all data and records."[35]

In 2002, the International Coalition of Library Consortia (ICOLC) issued "Privacy Guidelines for Electronic Resources Vendors," sending a clear message that

library privacy standards should also apply to library vendors. The introduction to ICOLC's privacy guidelines says they were issued "in the interest of informing the companies with which we do business about what is acceptable in the products and services we license." The guidelines include a suggested vendor privacy statement, which reads, in part: "We also believe it is critical for us to adhere to the American Library Association's *Code of Ethics*. We pledge to give you as much control as possible over your personal information. We will not disclose individually identifiable information about you to any third party without your consent."[36] ICOLC represents nearly 150 library consortia,[37] but—like ALA—has no formal authority over vendors. *Information Today* reported that the guidelines reflect the need for library consortia to "influence the practices of the vendor community on a global basis."[38]

Tables 2 and 3 list standards and guidelines gleaned from the above-cited documents of the International Coalition of Library Consortia and American Library Association. These standards, along with the Federal Trade Commission's "Fair Information Practice Principles," serve as the basis for this study's evaluation of vendor privacy policies.

TABLE 2
International Coalition of Library Consortia Guidelines (including content from the recommended sample policy)

- Publisher will have a written policy.
- Policy will be located on the online site.
- Policy should be easy to find.
- Policy should be easy to use/comprehensible.
- Policy should state that publisher adheres to ALA *Code of Ethics*.
- Policy should pledge that publisher will give user as much control as possible over their personal information.
- Policy should state that publisher will not disclose individually identifiable information about user to any third party without user's consent, except as required by law.
- Publisher will regularly review the functioning of the web site to ensure that its privacy policy is enforced and effective.
- Publisher will maintain full control over its site to prevent violation of privacy by a third party, such as advertiser or ISP.
- Publisher will not deny user access to its product on account of his/her election not to permit distribution of personal data to a third party.

Methodology

Target Population

The target population for the study was major vendors of electronic library databases, including indexing/abstracting/full-text resources and electronic journal packages, but not electronic book collections. Unfortunately, an extensive search yielded no existing list of vendors ranked by sales, market share, number of contracts, or other measure. Therefore, the following process was used to generate a list of major vendors.

First, the author reviewed the database holdings at her home institution and consulted with collection management librarians there to develop a preliminary list of 22 vendors. Then the author used data from the National Center for Education Statistics to identify 20 of the largest U.S. college and university campuses by enrollment.[39] Together, libraries at these institutions provide access to online resources to over 900,000 students. The author contacted the head acquisitions librarian at each of these institutions by telephone and asked if she or he would review the preliminary list and indicate whether or not she or he believed it represented the major vendors. "Major vendor" was defined as a vendor who offers what the librarian would consider one or more very important resources, or a vendor who offers a wide array of resources.

TABLE 3
American Library Association Policies, Interpretations, and Resolutions

"Policy on Confidentiality of Library Records":

- Library should adopt a policy that specifically recognizes that records identifying the names of users are confidential.

"Privacy: An Interpretation of the Library Bill of Rights":

- Library users have a right to be informed what polices and procedures govern the amount and retention of personally identifiable information.
- Library users have a right to be informed why collection of personally identifiable information is necessary.
- Library users have a right to be informed about what the user can do to maintain his or her privacy.

"Resolution on the Retention of Library Usage Records":

- Libraries should limit degree to which personally identifiable information is collected, monitored, disclosed, and distributed.
- Libraries should avoid creating unnecessary records.
- Libraries should ensure that records that must be retained are secure.
- Libraries should limit access to personally identifiable information to staff performing authorized functions.
- Libraries should dispose of library usage records containing personally identifiable information unless they are needed for the efficient and lawful operation of the library.
- Libraries should conduct an annual privacy audit to ensure that information processing procedures meet privacy requirements.

"Policy on Confidentiality of Library Records"; "Policy Concerning Confidentiality of Personally Identifiable Information About Library Users":

- Records identifying library users are not to be made available to any agency of state, federal, or local government, or other person except in response to a court order following a showing of good cause based on specific facts.

Of the 20 librarians contacted, 12 responded with feedback. Five vendors not on the preliminary list were mentioned by at least two librarians and were added. There was no agreement that any vendors should be deleted. This vetting process yielded a final list of 27 vendors considered to be major players by acquisitions librarians at the largest U.S. colleges and universities (table 4).

Sample

Because the target population of major vendors was a manageable number, no sampling was used. Rather, a census of the target population served as the pool for the study.

Data Collection and Analysis

The study used direct observation and content analysis to locate vendor privacy policies and measure them against standards articulated by the information technology industry and the library profession. The author first visited the online search page of a database published by each vendor and explored the links to see if a privacy policy was posted there. If no policy was found, the author contacted a vendor customer service representative, inquired about whether a policy was available, and, if so, requested a copy. If a policy was found, the author printed the policy, saved it as a text file, and recorded basic

facts about the policy, including the name of the link to the document, the number of clicks from the search page, and the date of last update. The author used Microsoft Word's "Word Count" and "Spelling and Grammar" tools to calculate word count, Flesch reading ease score, and Flesch-Kincaid grade level for each policy. The two latter measures attempt to quantify the readability of a text and were used to address the question of whether or not the policy is easy to understand. This discovery process provided immediate answers to some of the research questions. It also served to gather the text of policies for the formal content analysis described below.

TABLE 4
Major Vendors

1. Alexander Street Press
2. American Chemical Society
3. American Institute of Physics
4. CAB International
5. Cambridge University Press
6. CQ Press
7. EBSCO Information Services
8. Elsevier
9. Emerald Group Publishing Limited
10. Gale Cengage Learning
11. H. W. Wilson
12. HighWire Press
13. Ingenta
14. Institute of Electrical and Electronics Engineers (IEEE)
15. JSTOR
16. LexisNexis
17. Nature Publishing Group
18. NISC International, Inc.
19. OCLC Online Computer Library Center
20. Ovid Technologies
21. Oxford University Press
22. Project MUSE
23. ProQuest
24. Sage Publications
25. Springer
26. Thomson Reuters
27. Wiley-Blackwell

According to Neuendorf, "content analysis is a summarizing, quantitative analysis of messages that relies on the scientific method."[40] Berelson and Holsti indicate that content analysis may be used to compare content with a standard of adequacy or performance, but Holsti is critical of studies that use standards defined by the investigator's preferences.[41] That is not the case here. The standards are not the creation of the author; they have been published by the information technology industry and library profession.

When compared with techniques such as interview, Weber says, "content analysis usually yields unobtrusive measures in which neither the sender nor the receiver of the message is aware that it is being analyzed. Hence, there is little danger that the act of measurement itself will act as a force for change that confounds the data."[42] This makes it an especially appropriate research technique for evaluating vendors' promises regarding privacy. An interview or survey approach would likely yield less valid results, as vendor representatives who are eager to have their companies favorably perceived may be inclined to offer what they believe are acceptable responses.

Development of the Codebook

The author drafted a set of questions to be used as the codebook in the analysis of each vendor privacy policy, using the standards enumerated in tables 1, 2, and 3 as the basis for the questions. Two techniques were used to minimize the degree of judgment required by coders in using the codebook. First, all questions required nominal, not ordinal responses. According to Carney, "the very simplest kind of counting involves a mere check to see whether something is there or not."[43] Second, the codebook was designed to measure "manifest" or "on the surface" content, rather than "latent" content. The latter requires coders to make subjective interpretations based on their own mental schema.[44]

After creating the draft codebook, the author read through all the policies in the

pool to gain a sense of the language and construction used. Based on this knowledge, the author made revisions to the codebook and added coding instructions for questions that might cause confusion or uncertainty for coders. Both Neuendorf and Holsti recommend such immersion in the message pool as long as it precedes actual coding.[45]

Coder Training and Codebook Refinement

It is essential to have at least two coders to assess intercoder reliability and reproducibility, defined by Krippendorff as "the degree to which a process can be recreated under varying circumstances, at different locations, using different coders."[46] As Weber explains, "in content analysis, reliability problems usually grow out of the ambiguity of word meanings, category definitions, or other coding rules. Classification by multiple human coders permits the quantitative assessment of achieved reliability."[47] The process of assessing intercoder reliability is important because the goal of content analysis is to identify relatively objective message characteristics. Reliability measures indicate the extent to which a coding process will yield the same results on repeated trials and with different coders, and help to validate the coding scheme by making sure it is not limited to use by one individual.[48] Therefore, all policies in the pool were coded independently by two coders—the author and a second coder who is not a member of the library profession.

Considerable time was spent on coder training and refinement of the codebook. The author trained the second coder by reviewing with him the questions and coding instructions and discussing the meaning of various terms. To practice coding and identify areas of confusion, the author and the second coder then independently coded five library vendor privacy policies from *outside* the study pool. The two reviewed their results together, informally assessed the level of intercoder agreement, and discussed areas of disagreement. The author subsequently edited several questions and coding instructions for increased clarity, rearranged the order of questions, and made changes to the physical layout of the codebook. The two then tested the revised codebook by practice-coding a set of three library vendor privacy policies, also drawn from outside the study pool. An estimated 15 hours were spent in training, practice coding, and codebook revision. The codebook is available from the author.

Pilot Coding

Neuendorf and Lombard, Snyder-Duch, and Bracken[49] advise that reliability should be assessed at two points—a pilot before all coding is done and at a final stage after coding is finished. They also stress the importance of calculating intercoder reliability for *each* variable so that low reliabilities are not obscured by averaging across variables. The author and the second coder used the final revised codebook to independently code 10 vendor policies selected at random (using a random number generator) from *within* the study pool. After coding, percent intercoder agreement was calculated for each question/variable in this pilot to determine whether sufficient reliability was being achieved. For 19 variables, 100 percent agreement was achieved; for 12 variables, 90 percent agreement was achieved; for seven variables, 80 percent agreement was achieved. Agreement was below 80 percent for only two variables, at 70 percent and 60 percent.

Final Coding

Having achieved strong percent intercoder agreement for almost all variables, no further changes were made to the codebook, and the author and second coder proceeded with independent coding of the 14 remaining policies. (Three vendors had no policy.) All data were entered into a spreadsheet and percent intercoder agreement was recalculated for each variable. Because simple percent agreement is thought to be an "inappropriately liberal measure of intercoder

agreement,"[50] Perreault and Leigh's index of reliability (I_r) was used as a second measure of intercoder reliability.[51] Unlike crude percent agreement, this index takes into account the fact that some degree of agreement could be expected to occur simply by chance. Index of reliability (I_r) values range from zero to 1, with 1 indicating perfect agreement. Only variables that achieved intercoder reliability (I_r) scores of .80 and higher are reported and discussed. The author considered using the popular Cohen's kappa to measure intercoder reliability, but the nature of the data made it unworkable (ratings highly skewed toward one category; cases where there was no variability for one coder; and sometimes complete agreement between coders). For each instance in which the two coders disagreed, the author reviewed the variable and vendor policy in question and made a final determination about which answer—the author's or the second coder's—to include in the final data set.

Results and Discussion

Results are presented below in the five topical categories used by the FTC "Fair Information Practice Principles": 1) Notice/Awareness, 2) User Choice/Consent, 3) User Access/Participation, 4) Data Security, and 5) Enforcement/Redress. For each standard that was expressed in terms of what a privacy *policy* should say, policies were coded simply "yes" or "no." For other standards expressed in terms of what an *organization* should do, policies were coded "yes," "no," or "doesn't say." The "doesn't say" category allowed for the possibility that a vendor may follow a recommended practice but make no mention of it in its policy.

Notice/Awareness

Tables 5–7 present information about whether or not vendors have privacy policies, where the policies can be found, whether the policies bear a date and are easy to understand, and whether they explain what user information is collected and why. These questions were answered using direct observation, tools in Microsoft Word, and content analysis.

The vendors studied are doing a fair job meeting standards in the category "Notice/Awareness." Almost all (89%) have written privacy policies. Of these, 63 percent make their policies easy to find, available in one link from the database search page using unambiguous link names that include the word "privacy" (examples: "Privacy Policy," "Privacy & Security," "Privacy Policy and Legal Notices"). Only one policy was not available anywhere on the vendor's Web site; it was obtained by requesting a copy from a customer service representative. A strong majority (71%) of the policies include contact information or a link for questions, concerns, or more information about the policy.

All policies explain what user information is or may be collected, whether it be personally identifiable or anonymous and aggregated. All policies indicate that personal identifying information may be collected to provide certain services, and

TABLE 5
Vendor Policy Characteristics—Notice and Awareness
Existence, Currency, and Ease of Finding Policy

	Number of Vendors	Percent of Vendors
Vendor has written privacy policy (n=27)	24	89
Policy available one link away from search page (n=24)	15	63
Policy not available anywhere on vendor Web site (n=24)	1	4
Policy includes contact information for questions (n=24)	17	71
Policy includes date of last update (n=24)	6	25

TABLE 6 Vendor Policy Characteristics—Notice and Awareness Ease of Understanding Policy (n=24)	
Average length of policies	886 words
Average Flesch reading ease score of policies	39.2
Average Flesch-Kincaid grade level of policies	12

all policies state the purposes for which the information is gathered. Unfortunately, however, not a single policy mentioned or affirmed the ALA *Code of Ethics*, as recommended in the guidelines issued by ICOLC.

The policies ranged in length from 180 to 1,945 words, with an average of 886 words and a median of 863 words. The Flesch reading ease scores ranged from 26.3 to 54.8, with the average at 39.2. The Flesch reading ease index rates texts on a 100-point scale, with a higher number indicating greater reading ease. Scores ranging from 30 to 50 are considered "difficult" and typical of an academic journal; scores of 60 to 70 are considered "standard."[52] The Flesch-Kincaid grade level ranged from 10.1 to 12, with the average at 12. Only three (13%) policies scored lower than the 12th-grade level.

The scores suggest the policies are not easy to understand, but it is important to note that there is considerable debate about the validity of these indexes in assessing the comprehensibility of texts. Although objective and easy to apply, they take no account of the reader's interest and motivation, textual coherence, reader knowledge or perception,[53] or important variables such as paragraph length, organization, illogical propositions, misused words, and insufficient internal punctuation.[54] The Flesch formula is probably the most widely employed,[55] but because none of the available readability indexes is accepted as entirely valid or reliable,[56] readers should use caution in considering these results.

Beyond readability problems, users face a difficult challenge if they want to keep up with changes in vendor policy. Only six of the 24 policies (25%) include the date of last update, and eight (33%) include no information about potential updates or revisions to the policy. Sixteen policies (67%) do mention the possibility of updates and include language such as "changes will be effective when posted," "changes will appear on this page," and "check back to see changes," but only

TABLE 7
Vendor Policy Characteristics—Notice and Awareness
Information Collection Practices (n=24)

	Number of Vendors	Percent of Vendors	Percent Intercoder Agreement	Perreault & Leigh's Index of Reliability (I_r)	95% Confidence Lower Limit of I_r
Policy explicitly affirms ALA *Code of Ethics*	0	0	100	1	n/a
Policy explains what user information is/may be collected (*including none, aggregate, and/or personally identifiable*)	24	100	100	1	n/a
Vendor collects personal identifying information	24	100	100	1	n/a
Policy states why/for what purpose personal identifying information is collected	24	100	100	1	n/a

four of these 16 policies (25%) disclose the date of last update. It is, therefore, unclear how users would know if the policy had changed since they had last used the vendor's product, short of printing a copy of the policy and comparing the text word for word each time they returned to the vendor's Web site.

User Choice/Consent

Table 8 presents the results of content analysis that answered questions regarding user consent to vendors' collection and sharing of personal information and whether vendors give advice regarding how users can maintain privacy.

Vendors are doing less well expressing in policy a commitment to standards on user choice and consent. Although 92 percent of the policies offer advice (sometimes minimal) about how users can protect their privacy by avoiding certain features or making choices to "opt in" or "opt out," fewer than half (46%) of the policies say that the sharing of personal information is strictly voluntary and at the user's discretion. Only three policies (13%) explicitly label personal information as "confidential" or "private." One of these three policies later lists several situations in which the vendor *will* share information without the user's consent, leading one to wonder what was meant by "confidential."

Only five policies (21%) promise not to share personal identifying information with *any* third parties without user's consent. The remaining 19 policies express a variety of reasons for disclosure, but because they do not use consistent terminology, it was difficult to achieve adequate intercoder reliability on this variable. Reasons generally include protecting company property, for advertising and promotion purposes, to protect the safety of employees or the public, for the well-being of the company, and in relation to a legal proceeding. Several vendor policies acknowledge that personal information may be transferred as an asset in connection with a sale or merger of the company, thereby offering users no long-term protection. None of these 19 vendor policies explicitly promises to share information with third parties *only* with user's consent or in response to a court order, a standard set by ALA. Releasing information "in accordance to law" or "in response to a legal proceeding" is not the same as requiring a court order. It is unclear whether vendors are meeting the ICOLC standard of allowing users to access the product even if they elect not to allow distribution of personal identifying information; all but one policy were silent on this issue.

User Access/Participation

Table 9 presents the results of content analysis that answered questions about whether users are given the ability to control their personal information. This standard was measured by questions about whether users can view, change, and fully delete personal information held by vendors and remove their names from mailing/distribution lists.

Results regarding user access and participation are mixed. Close to three quarters of the vendor policies promise the user the ability to contest the accuracy or completeness of personal information held (71%) or have his/her name removed from distribution or mailing lists (79%). But only 29 percent of policies say the user has the ability to view the information held about him/her, and only 17 percent say the user can fully delete such information.

Data Security

Table 10 presents the results of content analysis that answered questions about avoiding the creation of unnecessary records, ensuring that retained records are secure, limiting staff access to personal information, and disposing of records no longer needed. The effort to measure compliance with one ICOLC standard in this area—"Publisher will maintain full control over its Web site to prevent violation of privacy by a third party, such as advertiser or ISP"—failed to achieve adequate intercoder reliability (I_r=.79), so it is not reported here. This was not

TABLE 8
Vendor Policy Regarding User Choice/Consent
(n=24, unless stated otherwise)

	Number of Vendors		Percent of Vendors	Percent Intercoder Agreement	Perreault & Leigh's Index of Reliability (I_r)	95% Confidence Lower Limit of I_r
Policy indicates how users can maintain their privacy (*includes advice about features to avoid or about opting in or opting out*)	22		92	92	.92	.81
Policy says giving of personal identifying information is strictly voluntary (*e.g., at user's discretion; knowingly provided by the user*)	11		46	83	.81	.66
Personal identifying information is explicitly labeled "confidential" or "private" in the policy (*beyond statements like "we endeavor to keep this information private" or "we respect your privacy"*)	3		13	92	.92	.81
Policy promises vendor will not share personal identifying information with ANY third parties (not including agents) without consent of user	5		21	100	1	n/a
Vendor shares personal identifying information with third parties ONLY in the following situations: with user's consent and/or in response to a court order (n=19)	Yes	0	0	95	.96	.89
	Doesn't Say	2	11			
	No	17	89			
If user elects not to permit distribution of their personal identifying data, vendor still allows access to product	Yes	0	0	88	.91	.79
	Doesn't Say	23	96			
	No	1	4			

surprising, as this standard caused the author and second coder a great deal of confusion during the practice coding. It is unclear what constitutes "full control."

Although most policies (79%) say the vendor takes steps to ensure the security of user records, the policies are generally silent on more specific standards related to data security. No policy says the vendor avoids creating unnecessary records, only one policy (4%) says vendor disposes of personal identifying records unless they're needed for lawful and efficient operation, and only six policies (25%) say vendor limits access to personal identifying information to staff performing authorized functions.

Enforcement/Redress

Table 11 presents the results of content analysis that answered questions about vendors' efforts to review their Web sites and information processing procedures to ensure that their policies are upheld and to offer a mechanism for policy enforcement and resolution of user complaints regarding privacy.

Vendor policies generally fail to address standards related to policy enforcement and redress. No vendor indicated in policy that it regularly reviews the functioning of its site to ensure that its privacy policy is enforced, and only one policy (4%) indicated that the vendor conducts a privacy audit of its information processing procedures (and does so "periodically"). Only two policies (8%) tell users how the policy is enforced or how complaints or policy violations will be addressed. It is interesting that not one of the 27 vendor search pages bears a third-party trust mark or privacy seal, such as TRUSTe, BBBOnline, WebTrust, or Better Web. Although this practice is not called for by the standards, it is one way a vendor could communicate its willingness to be accountable with regard to privacy and fair information practices.

Conclusion

This study found that the privacy policies of major vendors of online library resources fail to express a commitment to many of the standards articulated by the librarian profession and information technology industry for the handling and protection of user information. Vendors generally are providing notice about their information collection and sharing practices, but are doing little to let users control what happens to their personal information.

TABLE 9
Vendor Policy Regarding User Access/Participation (n=24)

	Number of Vendors		Percent of Vendors	Percent Intercoder Agreement	Perreault & Leigh's Index of Reliability (I_r)	95% Confidence Lower Limit of I_r
Vendor gives user ability to view, either online or by request, the personal information held about him/her (*ability not restricted or qualified in any way*)	Yes	7	29	83	.86	.73
	Doesn't say	14	58			
	No	3	13			
Vendor gives user ability to contest accuracy or completeness of personal information held	Yes	17	71	100	1	n/a
	Doesn't Say	7	29			
	No	0	0			
Vendor gives user ability to remove name from mailing/distribution list(s)	Yes	19	79	83	.86	.73
	Doesn't Say	5	21			
	No	0	0			
Vendor gives user ability to fully delete personal information	Yes	4	17	92	.94	.84
	Doesn't Say	19	79			
	No	1	4			

TABLE 10
Vendor Policy Regarding Data Security (n=24)

	Number of Vendors		Percent of Vendors	Percent Intercoder Agreement	Perreault & Leigh's Index of Reliability (I_r)	95% Confidence Lower Limit of I_r
Vendor avoids creating unnecessary personal identifying records	Yes	0	0	100	1	n/a
	Doesn't Say	24	100			
	No	0	0			
Vendor disposes of personal identifying records unless they are needed for efficient and lawful operation	Yes	1	4	92	.94	.84
	Doesn't Say	22	92			
	No	1	4			
Vendor takes steps to ensure security of records	Yes	19	79	96	.97	.90
	Doesn't Say	5	21			
	No	0	0			
Within its operations, vendor limits access to personal identifying information to staff performing authorized functions	Yes	6	25	88	.91	.79
	Doesn't Say	18	75			
	No	0	0			

They are unspecific in disclosing how they protect that information from unauthorized access or disclosure, and they offer no clear recourse for users who feel the terms of the policy have been violated. Also, it is clear from their policies that most vendors do not subscribe to the ALA *Code of Ethics* regarding the protection of user privacy and will share user information with third parties for a variety of reasons, some as vague as "to protect the well-being of the company." This is especially troubling in light of the fact that the government has drafted private industry for help in its data collection efforts.[57]

At the same time, the economic value of personal information is increasing. As Fister explains, corporations like Facebook and Google provide people with spaces to "play, engage with others, and make connections" in exchange for a chance to "gather data on what we think, do, read, say, and enjoy, and with whom we associate. It's exceedingly valuable information because it can be sold to companies who want to follow trends and focus their advertising dollars on just those individuals most likely to respond."[58] That's why Rupert Murdoch bought MySpace in 2005 for $580 million.[59] As Barnes observes, it's a "gold mine of market research; a microscope into the content habits and brand choices of America's capricious youth."[60] Librarians would be wise to remember that some of the vendors from whom they buy library databases are also in the business of selling personal information. For example, LexisNexis sells various marketing lists with titles such as "Consumer," "Homeowner," and "Relatives and Roommates." The LexisNexis database that generates these lists has records on over 225 million consumers and 118 million households "with a superior depth

TABLE 11
Vendor Policy Regarding Enforcement/Redress (n=24)

	Number of Vendors		Percent of Vendors	Percent Intercoder Agreement	Perreault & Leigh's Index of Reliability (I_r)	95% Confidence Lower Limit of I_r
Vendor regularly reviews functioning of its site to ensure that privacy policy is enforced and effective	Yes	0	0	96	.97	.90
	Doesn't Say	24	100			
	No	0	0			
Vendor conducts a privacy audit to ensure that information processing procedures meet privacy requirements	Yes	1	4	96	.97	.90
	Doesn't Say	23	96			
	No	0	0			
Policy explains how the policy is enforced or the mechanism through which complaints and breaches will be addressed (*beyond simply providing contact information for questions*)	2		8	96	.96	.88

of demographic and lifestyle indicators," according to LexisNexis.[61] Other vendors, such as EBSCO Publishing, belong to parent companies whose mission is vastly different from that of the library. EBSCO Industries is a conglomerate that includes a fishing lure manufacturer, a specialty office and computer furniture retailer, a real estate company, and a rifle manufacturer.[62]

As more companies recognize the economic value of collecting, retaining, and selling personal information, librarians are likely to see greater efforts on the part of vendors to solicit information from library users. Such efforts may be presented as features designed for the convenience of the library user (for example, save favorite searches or articles), and they may indeed provide greater convenience; but this study shows that vendors do not presently share librarians' commitment to privacy. This is especially important given Hsu's research showing that the online privacy behavior of university students is influenced by social contexts and Web site categories,[63] and the finding of De Rosa et al. that libraries are viewed as trustworthy.[64] Students who trust the library and its promise of confidentiality may be inclined to divulge personal information while using databases offered by the library. If librarians are to remain true to the *Code of Ethics* and the principles that distinguish libraries as special places for free and open inquiry, they must carefully examine the policies behind those databases, advocate for the protection of user privacy, and educate users who have placed their trust in the library.

Limitations and Recommendations for Further Research

While the study took a scientific approach to understanding the content of library vendor privacy policies, it does not measure actual practice of these vendors. It does not assess the degree to which vendors are committed to upholding the

promises they make in their policies nor the extent to which they have upheld them in the past. As Holsti cautions, content analysis "can rarely be used to determine the truth of an assertion."[65] The study is also limited by its focus on the policies of major library vendors, following the logic that the online products of these vendors—and therefore their privacy practices—touch a vast number of college and university library users. It would be interesting to replicate the study with other groups of vendors and to compare and contrast the results.

It would be valuable to find a more meaningful way to measure readability of policies, and—though undoubtedly difficult to do—it also would be interesting to ask vendor representatives to code their own policies and compare the results with those reported here. Would vendors interpret their own policies differently? Also, the present study did not address vendors' use of Web beacons, clear GIFs, and cookies, all of which may have implications for user privacy.

Finally, before an appropriate course of action can be determined, it is important to learn whether acquisitions and collection librarians have made or are making any demands concerning user privacy in their negotiations with vendors. If they have not, why not? If they have, what have been the results of those efforts?

Notes

1. Judith Krug, "History—Code of Ethics," in *Intellectual Freedom Manual*, 7th ed., ed. American Library Association, Office for Intellectual Freedom (Chicago: American Library Association, 2006), 246–65.
2. John A. Drobnicki, "The Confidentiality of Library Users' Records" (ERIC Document Reproduction Service, No. ED358846, 1992).
3. Arthur W. Hafner and Jennifer Sterling-Folker, "The American Public Library and the Constitutional Right to Freedom of Expression," in *Democracy and the Public Library*, ed. Arthur W. Hafner (Westport, Conn.: Greenwood, 1993), 105–72.
4. Stacey L. Bowers, "Privacy and Library Records," *Journal of Academic Librarianship* 32, no. 4 (2006): 380.
5. David Burnham, *A Law unto Itself: Power, Politics, and the IRS* (New York: Random House, 1989), 87–88; Judith Krug, "ALA and Intellectual Freedom—A Historical Overview," in *Intellectual Freedom Manual*, 7th ed., ed. American Library Association, Office for Intellectual Freedom (Chicago: American Library Association, 2006), 21–22.
6. Bill McAllister, "Librarians Want FBI to Shelve Requests about Foreign Readers: Agency Faulted for Asking Information about Book-Borrowers," *Washington Post*, Mar. 27, 1988. Available online at www.lexisnexis.com. [Accessed 18 June 2007].
7. Mary Minow and Tomas A. Lipinski, "Library Records and Privacy," in *The Library's Legal Answer Book* (Chicago: American Library Association, 2003), 169; Theresa Chmara, "State Privacy and Confidentiality Statutes," in *Privacy and Confidentiality Issues: A Guide for Libraries and Their Lawyers* (Chicago: American Library Association, 2009), 43–44.
8. Samuel J. Best, Brian S. Krueger, and Jeffrey Ladewig, "The Polls—Trends: Privacy in the Information Age," *Public Opinion Quarterly* 70, no. 3 (2006): 375–401.
9. Cathy De Rosa et al., *Sharing, Privacy and Trust in Our Networked World: A Report to the OCLC Membership* (Dublin, Ohio: OCLC, 2007). Available online at www.oclc.org/reports/sharing/default.htm. [Accessed 21 January 2009].
10. Karen McCullagh, "Blogging: Self Presentation and Privacy," *Information & Communications Technology Law* 17, no. 1 (2008): 3–23.
11. Andrew Romano, "Facebook's 'News Feed,'" *Newsweek*, Sept. 25, 2006. Available online at www.lexisnexis.com. [Accessed 11 June 2007].
12. Abbey Klaassen, "Egg on Their Facebook: Users Force Reversal of Ad Approach," *Advertising Age*, Dec. 3, 2007. Available online at www.lexisnexis.com/us/lnacademic. [Accessed 21 January 2009].
13. Andrew LaVallee, "Recapping the Three-Day Facebook Firestorm," *Digits* [a *Wall Street Journal* blog], Feb. 18, 2009, available online at http://blogs.wsj.com/digits/2009/02/18/recapping-the-three-day-facebook-firestorm/ [Accessed 19 February 2009]; Jessica E. Vascellaro, "Facebook's About-Face on Data," *Wall Street Journal*, Feb. 19, 2009, available online at http://wsj.com [Accessed 19 February 2009].

14. Emily Nussbaum, "Say Everything," *New York,* Feb. 12, 2007, 24–29 and 102–03.

15. Steven Johns and Karen Lawson, "University Undergraduate Students and Library-Related Privacy Issues," *Library & Information Science Research* 27 (2005): 485–95.

16. Seounmi Youn, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media* 49, no. 1 (2005): 86–110.

17. Deborah M. Moscardelli and Richard Divine, "Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors," *Family and Consumer Sciences Research Journal* 35, no. 3 (2007): 247.

18. Amanda Lenhart and Mary Madden, *Teens, Privacy & Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace* (Pew Internet & American Life Project, Apr. 18, 2007). Available online at www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx. [Accessed 21 January 2009].

19. Chiung-wen (Julia) Hsu, "Privacy Concerns, Privacy Practices and Web Site Categories: Toward a Situational Paradigm," *Online Information Review* 30, no. 5 (2006): 569–86; Carlos Jensen, Colin Potts, and Christian Jensen, "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies* 63, no. 1/2 (2005): 203–27; Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* 41, no. 1 (2007): 100–126; Carina Paine et al., "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions,'" *International Journal of Human-Computer Studies* 65, no. 6 (2007): 526–36; Evelien van de Garde-Perik et al., "Investigating Privacy Attitudes and Behavior in Relation to Personalization," *Social Science Computer Review* 26, no. 1 (2008): 20–43.

20. Susan B. Barnes, "A Privacy Paradox: Social Networking in the United States," *First Monday* 11, no. 9 (2006). Available online at http://firstmonday.org/issues/issue11_9/barnes/index.html. [Accessed 9 July 2007].

21. Edward M. Corrado, "Privacy and Library 2.0: How Do They Conflict?" in *Sailing Into the Future: Charting Our Destiny: Proceedings of the Thirteenth National Conference of the Association of College and Research Libraries, March 29–April 1, 2007, Baltimore, Maryland*, ed. Hugh Thompson (Chicago: ACRL, 2007), 333.

22. Judy Luther, *White Paper on Electronic Journal Usage Statistics* (Washington, D.C.: Council on Library and Information Resources, 2000), 12–13.

23. Jeannette Woodward, "The Challenge of Library Records: What to Keep and How Long to Keep It," in *What Every Librarian Should Know about Electronic Privacy* (Westport, Conn.: Libraries Unlimited, 2007), 128–29.

24. Rory Litwin, "The Central Problem of Library 2.0: Privacy," in *Library Juice Concentrate*, ed. Rory Litwin (Duluth, Minn.: Library Juice Press, 2006), 71–74.

25. Paul Sturges et al., "User Privacy in the Digital Library Environment: An Investigation of Policies and Preparedness," *Library Management* 24, no. 1 (2003): 49.

26. "ICOLC Releases Privacy Guidelines," *Information Today* 19, no. 8 (2002). Available online at http://web.ebscohost.com [Academic Search Premier database]. [Accessed 4 December 2008].

27. Primary Research Group, Inc., *Survey of Library Database Licensing Practices*, 2008 ed. (New York: PRG, 2008).

28. Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, Sept. 23, 1980). Available online at www.oecd.org/documentprint/0,3455,en_2649_34255_1815186_1_1_1_1,00.html. [Accessed 10 October 2008].

29. Federal Trade Commission. *Fair Information Practice Principles* (Washington, D.C., June 25, 2007). Available online at www.ftc.gov/reports/privacy3/fairinfo.shtm. [Accessed 13 November 2008].

30. TRUSTe, *Your Online Privacy Policy—An Informational Paper About Drafting Your First Privacy Statement or Improving Your Existing One* (2004), 3. Available online at www.truste.org/ (click "Privacy Policy Whitepaper"). [Accessed 7 November 2008].

31. Council of the American Library Association, *Privacy: An Interpretation of the Library Bill of Rights* (American Library Association, June 19, 2002). Available online at www.ala.org/ala/aboutala/offices/oif/statementspols/statementsif/interpretations/privacy.cfm. [Accessed 10 November 2008].

32. Council of the American Library Association, *Policy on Confidentiality of Library Records* (American Library Association, July 2, 1986). Available online at www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13084. [Accessed 10 November 2008].

33. Council of the American Library Association, *Policy Concerning Confidentiality of Personally Identifiable Information About Library Users* (American Library Association, June 30, 2004). Available online at www.ala.org/Template.cfm?Section=otherpolicies&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13087. [Accessed 10 November 2008].

34. Council of the American Library Association, *Resolution on the Retention of Library Usage Records* (American Library Association, June 28, 2006). Available online at www.ala.org/ala/

aboutala/offices/oif/statementspols/ifresolutions/ALA_print_layout_1_388477_388477.cfm. [Accessed 10 November 2008].

35. Council of the American Library Association, *Policy Concerning Confidentiality*; Council of the American Library Association, *Resolution on the Retention of Library Usage Records*.

36. International Coalition of Library Consortia, *Privacy Guidelines for Electronic Resources Vendors* (July 2002). Available online at www.library.yale.edu/consortia/2002privacyguidelines.html. [Accessed 24 September 2008].

37. International Coalition of Library Consortia, *About the International Coalition of Library Consortia* (Dec. 2, 2007). Available online at www.library.yale.edu/consortia. [Accessed 10 October 2008].

38. "ICOLC Releases Privacy Guidelines."

39. National Center for Education Statistics, "Table 225. Enrollment of the 120 Largest Degree-granting College and University Campuses, by Selected Characteristics and Institution: Fall 2005," in *Digest of Education Statistics* (2007). Available online at http://nces.ed.gov/programs/digest/d07/tables/dt07_225.asp. [Accessed 23 September 2008].

40. Kimberly A. Neuendorf, *The Content Analysis Guidebook* (Thousand Oaks, Calif.: Sage Publications, 2002), 10.

41. Bernard Berelson, *Content Analysis in Communication Research* (New York: Hafner, 1971), 190–91; Ole R. Holsti, *Content Analysis for the Social Sciences and Humanities* (Reading, Mass.: Addison-Wesley, 1969), 31.

42. Robert Philip Weber, *Basic Content Analysis*, 2nd ed. (Newbury Park, Calif.: Sage, 1990), 10.

43. Thomas F. Carney, *Content Analysis: A Technique for Systematic Inference from Communications* (Winnipeg: University of Manitoba Press, 1972), 150.

44. Matthew Lombard, Jennifer Snyder-Duch, and Cheryl Campanella Bracken, *Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects* (Oct. 3, 2008). Available online at www.temple.edu/sct/mmc/reliability/. [Accessed 2 December 2008].

45. Neuendorf, *The Content Analysis Guidebook*, 72; Holsti, *Content Analysis*, 11.

46. Klaus Krippendorff, *Content Analysis: An Introduction to Its Methodology* (Beverly Hills, Calif.: Sage, 1980), 131.

47. Weber, *Basic Content Analysis*, 15.

48. Neuendorf, *The Content Analysis Guidebook*, chap. 7; Lombard, Snyder-Duch, and Bracken, *Practical Resources*.

49. Ibid.

50. Lombard, Snyder-Duch, and Bracken, *Practical Resources.*

51. William D. Perreault Jr. and Laurence E. Leigh, "Reliability of Nominal Data Based on Qualitative Judgments," *Journal of Marketing Research* 26, no. 2 (1989): 135–48.

52. Rudolf Flesch, "A New Readability Yardstick," *Journal of Applied Psychology* 32, no. 3 (1948): 230.

53. Michael B.W. Wolfe, "Readability Indices," in *Encyclopedia of Education*, 2nd ed., ed. James W. Guthrie, vol. 6 (New York: MacMillan Reference USA, 2003), 1972–73; Bradford R. Connatser, "Last Rights for Readability Formulas in Technical Communication," *Journal of Technical Writing and Communication* 29, no. 3 (1999): 271–87.

54. Annette Shelby, "Readability Formulas: One More Time," *Communication Forum* 5, no. 4 (1992): 485–95.

55. Wolfe, "Readability Indices," 1972.

56. "Readability," in *Encyclopedia of American Education*, 2nd ed., ed. Harlow G. Unger, vol. 3 (New York: Facts on File, 2001): 881.

57. Rachel Friedman, "Protecting Customer Privacy," *Information Today* 25, no. 1 (2008), available online at http://web.ebscohost.com [Academic Search Premier database] [Accessed 31 March 2009]; Eric Lichtblau, "FBI Data Mining Reached Beyond Initial Targets," *New York Times*, Sept. 9, 2007, available online at http://www.lexisnexis.com [Accessed 31 March 2009].

58. Barbara Fister, "Face Value," *Inside Higher Ed,* Feb. 18, 2008. Available online at www.insidehighered.com/layout/set/print/views/2008/02/18/fister. [Accessed 21 February 2008].

59. Richard Wray, "Social Networking: Facebook Challenges MySpace as Place for the Cool Set to Hang Out: Helping People Stay in Touch with Friends Online has Become the Latest Battleground for Moguls," *Guardian*, June 21, 2007. Available online at www.lexisnexis.com. [Accessed 17 July 2007].

60. Barnes, "A Privacy Paradox."

61. LexisNexis, "Lists." Available at http://risk.lexisnexis.com/acquire-new-customers. [Accessed 23 March 2009].

62. Amy Schein, "EBSCO Industries Inc.," in *Hoover's Company Records* (Mar. 15, 2009). Available online at http://proquest.umi.com. [Accessed 18 March 2009].

63. Hsu, "Privacy Concerns."

64. Cathy De Rosa et al., *Sharing, Privacy and Trust.*

65. Holsti, *Content Analysis*, 18.