IOWA STATE UNIVERSITY
Digital Repository

Collections and Technical Services Publications and Papers

Collections and Technical Services

Fall 2005

University undergraduate students and library-related privacy issues

Steven Johns
Iowa State University

Karen G. Lawson
Iowa State University, klawson@iastate.edu

Follow this and additional works at: http://lib.dr.iastate.edu/libcat_pubs

 Part of the Library and Information Science Commons

The complete bibliographic information for this item can be found at http://lib.dr.iastate.edu/libcat_pubs/27. For information on how to cite this item, please visit http://lib.dr.iastate.edu/howtocite.html.

This Article is brought to you for free and open access by the Collections and Technical Services at Iowa State University Digital Repository. It has been accepted for inclusion in Collections and Technical Services Publications and Papers by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

University undergraduate students and library-related privacy issues

Abstract
New technologies increase the ability to capture and retrieve data about library usage patterns and users. Collecting, analyzing, and using patron data, however, may raise concerns among library users about their online privacy and how the data collected might be used to their advantage or disadvantage. This article examines undergraduate students' knowledge and perceptions of online privacy issues, their opinions regarding who should collect and retain information about them, for what purposes, and under what circumstances.

Disciplines
Library and Information Science

Comments
This is a post-print of an article from *Library & Information Science Research*, 27, no. 4 (Autumn 2005): 485–495, http://dx.doi.org/10.1016/j.lisr.2005.08.006.

This article is available at Iowa State University Digital Repository: http://lib.dr.iastate.edu/libcat_pubs/27

University Undergraduate Students and Library-related Privacy Issues

Steven Johns
Assistant Professor
Iowa State University Library
Ames, Iowa 50011
sljohns@iastate.edu

Karen Lawson
Associate Professor
Iowa State University Library
Ames, Iowa 50011
klawson@iastate.edu

ABSTRACT

New technologies increase the ability to capture and retrieve data about library usage patterns and users. Collecting, analyzing, and using patron data, however, may raise concerns among library users about their online privacy and how the data collected might be used to their advantage or disadvantage. This article examines undergraduate students' knowledge and perceptions of online privacy issues, their opinions regarding who should collect and retain information about them, for what purposes, and under what circumstances.

1. Introduction

Internet users are concerned about protection of their online privacy. Marcella and Stucki (2003, p. 241) report that the problem is increasing as Internet addresses can now be linked to actual identities. The nature of the Internet causes information to pass through dozens of networks and computer systems, each with some ability to capture and store information about online activities. Private corporations and government are two groups who may be most commonly perceived as making use of this opportunity for transactional analysis.

There are arguments to be made for both the benefits and detriments of user-transaction monitoring in libraries. Nicholson and Stanton (2004, p. 247) describe ways that "bibliomining" can be used to understand patterns of behavior among library users and staff members and patterns of information resource use within a library. They find it unfortunate that few libraries have taken advantage of available data as a way to improve customer service, manage acquisition budgets, or influence the way policies for information use are chosen. Estabrook's (1996, p. 48) aptly titled article "Sacred Trust or Competitive Opportunity: Using Patron

Records," advocates for the use of patron data to improve library services. She notes that libraries provide searching tools that allow users to target their needs more effectively and libraries should use information from those tools to target users' needs more effectively. Estabrook (1996, p. 49) writes: "We can create 'communities of interest' by grouping our users. Then we can use the network to expand our services across space and time."

Estabrook, Nicholson, and Stanton agree that there are caveats that should accompany user-transaction monitoring. Nicholson and Stanton (2004, p. 257) advise organizations to develop a careful balance between discovering usage patterns and connecting those patterns to particular individuals in the system. Estabrook (1996, p. 49) recommends the preemptive action of getting informed consent from users along with compiling user data that could be encrypted in some way that would conceal the name of the user, including from staff, but would compile aggregate demographic statistics. Rezmierski and Seese (2002) write:

> As institutions of higher education carry out more of their business and mission over networked information infrastructures, it is increasingly important to provide a secure environment for individual and corporate data. Three aspects of security must be ensured: confidentiality, validity, and integrity. Confidentiality is important because academic environments are places of exploration and inquiry. (p. 3)

Librarians also have had the ability for several decades to capture information about library users' interest in library resources via in-house monitoring of their circulation histories. More recently, data monitoring has expanded to include the ability to capture and retain online search histories. Library managers can use their data to track common patterns of user behavior to aid in decision-making processes. By example, analysis of user behavior patterns offers the opportunity to provide focused services and collections targeted to particular groups of library users. With the proliferation of electronic resources available through library Web sites, data

analysis can be used to learn more about users' needs. This type of analysis, however, may raise concerns among library users about their online privacy and how the data collected might be used to their advantage or disadvantage.

Library user information has not always been protected. Estabrook (1996) describes patron circulation information visible to anyone viewing a signed a book card for a particular volume. Foerstal, (1991), and Nicholson and Stanton (2004) detail the Federal Bureau of Investigations' (FBI) history of monitoring of library data and users. In response, the American Library Association (ALA) and librarians across the country have lobbied for laws that protect user records in libraries (Stielow, 1993, p. 710). These laws vary in their scope and protection, however, and internal use of user information for library management is usually permitted. Libraries can use patron records to support the mission of the library, but third parties are usually proscribed from viewing this information. The current "Code of Ethics" of the American Library Association (1995) states: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted." As a result, users generally perform research in libraries with a sense of security.

The Family Educational Rights and Privacy Act of 1974 (FERPA), along with other legislation, further protected the privacy of education-related records. Some information, however, was considered public and could be released to anyone unless the student notified the university that they did not wish the information be released. Information that could be released without a student's permission included the student's name, telephone number, e-mail address, major field of studies, and dates of attendance. Students have rights pertaining to the personal information a university can release, but may lack knowledge of and require information about

how to "opt out" of the release of information. Students' ability to, or likelihood of, opting out could depend on how aggressive the university is in informing the students about FERPA, or how aware the student is of the policy.

Educators often make attempts to safeguard their students' online activity. They write and speak about online privacy and safety issues in an attempt to teach students how to use technologies in a way that is both ethical and responsible (Crystal, Geide, Salpeter, 2000, p. 27). Hoffman and Spencer (2000, p. 6) developed a curriculum on privacy that provides an explanation of what privacy is, how privacy relates to people's lives, how violations of personal privacy can influence people's futures, and the rights and responsibilities involved in the protection of personal privacy.

In 2001, Congress passed the USA PATRIOT Act, which contains Section 215, that obliges librarians**,** if requested**,** to cooperate with federal agents by turning over the records identifying resources specific library users have searched or checked out of the library. Certainly, online privacy was an important issue to libraries and their users prior to the PATRIOT Act. Saftner and Raghunathan (1995, p. 43) questioned why people feel that privacy is important enough to be concerned about and why they think that their privacy is being threatened. More recently, VanScoy and Oakleaf (2003) wrote:

> Librarians find themselves now in a delicate balancing act. On one hand, they struggle to create new services that patrons will find exciting and useful. On the other hand, they champion privacy rights that many patrons don't value. With the current political climate, online privacy is likely to become a more volatile topic. As patrons become more aware of the issues, they may begin to make their concerns and preferences known. Even with this valuable input from patrons, more research will be needed to determine where the acceptable tradeoff is between online privacy and enhanced virtual reference. (p.6)

Librarians and educators are aware of issues pertaining to user confidentiality. What is less known are the perceptions that various segments of the population, such as incoming university students, have about the policies, legislation, and practices that may affect them. If a library develops, implements, and disseminates a privacy policy, does anyone have the responsibility to read it?

Now, as potential reporters of that information to government entities under the PATRTIOT Act, librarians may have an obligation to study what patrons know about the information that is being captured by library systems. While some librarians might agree that the collection and analysis of user information to influence library decision-making is acceptable, does the student user community agree? Would students also agree that it is acceptable to target specific groups of library users based on transactional information to better market library services? This article reports on the results of a survey of university library student users and their awareness, knowledge, and concerns regarding online privacy.

2. Problem Statement

Librarians have long been custodians of information about library usage. New technologies increase the ability of librarians to capture and retrieve data about users. The PATRIOT Act legislation caused a re-examination of library confidentiality policies nationwide. Due to the PATRIOT Act, librarians are now also potential reporters of such information to government agencies. There is little available literature about undergraduate students' knowledge and perceptions of online privacy issues, their opinions regarding who should collect and retain information about them, for what purposes, and under what circumstances. Students

may be unaware of these issues. Do librarians have a duty to inform them? Would students also agree that it is acceptable to target specific groups of library users based on transactional information to better market library services? To better serve and protect library users, university librarians need a better understanding of undergraduate students' knowledge and perceptions about library-related privacy issues.

3. Methodology

Between August 25, 2003, and January 14, 2004, the authors surveyed 444 students at Iowa State University (ISU) enrolled in ISU's required library orientation course, Library 160, about their:

- Knowledge of the types of information their library may store online
- Familiarity with legislation that might require the library to provide some of that information to entities outside the university
- Opinions about potential legitimate reasons for collecting, and using, that information

Library 160 is a seven-week course offered during various sessions throughout the academic year. The students were surveyed during the fall of 2003 and the spring of 2004. Four groups of Library 160 students were surveyed, including Honors Program students who complete the program as a discrete group. Successful completion of this course is a university requirement. Its curriculum focuses on the use of libraries and information sources, both print and electronic, including locations and services of the ISU Library with an emphasis on the research process. The University recommends that the course be taken as early as possible in the student's undergraduate career. The survey focused on student knowledge and concerns about

online privacy issues, and what part librarians might have, if any, in informing students about the types of captured information and uses or potential uses of that information.

Library 160 students are primarily freshmen (73% over the past five years). Their knowledge and opinions of these issues provide a "baseline" of what the least experienced, and potentially most at-risk, students think and know. The questionnaire was composed of 31 questions which sought to assess student knowledge and concerns regarding privacy of personal information online. The questions included: two demographic questions, one question on computer literacy and skills, one question about the ISU's "Code of Computer Ethics and Acceptable Use Policy" (Iowa State University, 2004), seven questions about the PATRIOT Act and how it might affect online privacy, and 20 questions about knowledge and opinion of online privacy issues. At the end of the survey, students were given a space for free commentary about computer privacy. The survey package consisted of the questionnaire, a standard bubblesheet answer sheet, and an instruction/consent letter. The letter accompanying the survey included instructions and a statement that the survey was entirely voluntary, completely anonymous, and would in no way affect the student's Library 160 grade.

[insert Table 1 here]

The surveys were conducted during the Library 160 introductory lecture, except for the Honors Program students who were given the opportunity to take the survey after they had completed the course final exam. The purpose for the survey was explained to the students, and the instructions reinforced. Table 1 shows that, for the three non-honors groups, case response was quite high. A smaller percentage, (54%, n=86) of Honors students elected to take the survey. Overall however, for all four groups, survey response was fairly high at (81%, n=444).

There was occasional item non-response (i.e., no answer marked on the survey instrument). Item non-response was negligible, averaging less than one non-response per each question, per each group surveyed. Due to rounding practices of the ISU Testing and Evaluations Service software, total percentages for some questions do not equal 100%.

The ISU Honors Program student group was unique among the groups surveyed for several reasons. They were the only group not surveyed during the Library 160 introductory lecture. Honors students do not attend an introductory lecture. They independently study the course manual, complete the five course assignments, and then take the same final exam that other Library 160 students take. The final exam represented the only access to this group and they were surveyed after taking the exam. This method resulted in a lower rate of surveys captured. Of the 158 honors students given the opportunity to take the survey, 86 students, (54%), chose to do so. Thus self-selection bias was higher for the Honors student group than for the other three groups surveyed.

4. Results

Of the 444 students who participated, (77%, n=339) were freshman, and (4%, n=19) were graduate students, the smallest segment. A large majority (97%, n=429) of the students had lived most of their life in the United States. Students were questioned about the level of their computer skills to evaluate whether there was a correlation between those skills and their knowledge about privacy-related issues. They were asked to rank their computer skills at one of three skill levels. Most students (45%, n=201) chose the middle skill level: "I use the computer a lot and know several different programs such as (Microsoft's) Excel or FrontPage." Sixty-eight percent (n=302) of the students considered themselves having more than simple computer skills.

Having a good grasp of computer skills did not correspond to having detailed knowledge about privacy-related information. Ninety-four percent (n=467) were only somewhat or not at all familiar with ISU's "Code of Computer Ethics and Acceptable Use Policy" and 94% (n=418) were only somewhat or not at all familiar with the PATRIOT Act.

Iowa State University's "Computer Code of Ethics and Acceptable Use Policy" is available online on ISU's Web site in the University's Policy Library, but it is not distributed to incoming students in any way. The policy "provides for access to information technology resources and communications networks within a culture of openness, trust, and integrity. In addition, Iowa State University is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems" (Iowa State University, 2004, Introduction, para. 1). The Computer Code is mentioned in, but not included in the text of, the ISU *Student Information Handbook*. A keyword search of the ISU Web site revealed several versions of the Code, published on pages ranging from ISU academic departmental pages to the course pages for an ISU course on philosophy and ethics. However, the Computer Code states that "every user of university IT resources is required to know the policies and to conduct their activities within the scope of the ISU Code of Computer Ethics and Acceptable Use Policy, the ISU Information Technology Security Policy, and the Standards, Guidelines, and Best Practices for IT Security. Failure to comply with this policy may result in loss of computing privileges and/or disciplinary action" (Iowa State University, 2004, Introduction, para. 6). When questioned about their familiarity with the ISU's "Code of Computer Ethics and Acceptable Use" only (6%, n=27) of ISU students were "very familiar" with the Code and (41%, n=183) were "somewhat familiar" with it. Fifty-three percent (n=234)

were “not familiar” with the Code.

[insert Table 2 here]

Another group of survey questions dealt with “PATRIOT Act” legislation. Only (6%, n=25) responded that they were “very familiar” while (26%, n=116) were “somewhat familiar” with it. A large proportion, (68%, n=302) of students surveyed, were not familiar with the “PATRIOT Act.”

Students who had some familiarity with the Act were then asked where they had first heard about it. They were also queried about whether they thought the Act might affect their online privacy, the privacy of their library records, their use of library resources, and their use of library computer workstations.

Most students, (42%, n=81) who were familiar or very familiar with the PATRIOT Act, first heard about the Act through radio or television. The Internet, (7%, n=14) was the least likely place students had first heard of the legislation. Students overwhelmingly (84%, n=158) agreed that the Act might affect their online privacy. Sixty-six percent (n=121) of students thought the Act could affect use of their library records (borrowing records for example). Most students also felt that the Act could affect monitoring their use of library resources (78%, n=146) and their use of library computer workstations (83%, n=150).

The purpose of another of questions on the survey was to gauge the circumstances under which students thought the University, or more specifically the library, might justifiably look at their online transactions. Of the total number of students responding, (62%, n=274) felt virus prevention/flushing constituted justifiable use of private information; and (58%, n=255) felt tracking and prosecuting unauthorized computer users and aiding law enforcement officers with

a search warrant were just causes. Fewer students (38%, n=167)) felt violations of ISU's "Code of Computer Ethics and Acceptable Use" or managing and distributing computer bandwidth (25%, n=111) constituted sufficient cause to look at their online private information. Even fewer students (23%, n=104) felt that developing student profiles for the purpose of enhancing the Library's collection and services constituted justifiable use. Finally, (32%, n=140) of students surveyed felt "there is no reason a University or Library can justifiably look at a student's private information."

[insert Table 3 here]

Students were asked: "How important is online privacy to you?" While (1%, n=4) were undecided and (4%, n=18) did not think it was important, (95%, n=422) of students felt online privacy held some importance to them. Specifically, (51%, n=225) answered "very important," (34%, n=152) answered "important," and (10%, n=45) answered "somewhat important." Responses to this question were also analyzed for Freshmen only and for Seniors only, with responses for each class being essentially identical to the responses of the survey population as a whole. The following table shows responses for the whole survey population.

[insert Table 4 here]

Students were asked who, other than themselves, should have access to certain types of private information. Students were to select between two answers: "ISU Network security officials" (ISUNS) and "no one." Eighty-nine percent (n=394) felt ISUNS could have access to general information such as their e-mail or campus address. A little over half (54%, n=240) of the students felt ISUNS could have access to their student ID number. Percentages begin to fall

off sharply, however, for ISUNS access to grades (23%, n=102), web surfing habits (13%, n=59), and e-mail message content (7%, n=29).

The survey asked students to indicate their degree of agreement or disagreement to a set of varied questions regarding their online privacy. Ninety-two percent (n=406) agreed or strongly agreed that a university or library should only try to obtain private information with students' informed consent. Eight-six percent (n=380) agreed or strongly agreed that a university or library should only collect information for clearly defined purposes. Ninety-one percent (n=403) agreed or strongly agreed that a university or library should never disseminate students' personal information to outside agencies. Seventy-four percent (n= 328) of students agreed or strongly agreed that a university or library should assign appropriate life spans to the retention of private student information. Seventy-eight percent (n=346) of students agreed or strongly agreed that the library should take responsibility for informing students about "The PATRIOT Act."

[insert Table 5 here]

Two survey questions asked students how well they thought the ISU Library protected their online privacy and how they thought the ISU Library kept them informed of efforts to protect their online privacy. Forty-eight percent (n=212) of students thought the Library was doing fairly well or extremely well in protecting student online privacy, but many (41%, n=183) were undecided about how well the library was performing this function. Seventy-six percent (n=337) of students felt that the Library was either not doing a good job of keeping students informed of efforts to protect their online privacy or were undecided about the job the Library was doing in this area.

At the end of the survey, students were given space for free commentary about online privacy issues or concerns. Members of the Honors group were most likely to take advantage of this opportunity. The comments revealed that the students felt there is no privacy online and people should not expect or think that there is, and that the ISU Library should only access students' private information with students' permission or a search warrant.

5. Discussion

Electronic information networks offer many advantages in terms of power, capacity, speed, accessibility, and cost. Organizations and individuals are able to collect and use data available in digital format. These capabilities present substantial privacy issues. While no statistics available in the literature give a clear indication on how many libraries collect and/or use patron usage information for collection development, marketing, or other purposes, the potential for usage exists and grows easier with technological advances.

ISU students do not view enhancing the Library's collection and services as sufficient cause for using private information about them. Seventy-seven percent (n=339) of students felt developing student profiles for the purpose of enhancing the library's collection and services did not constitute justifiable use of online student information. When presented with seven scenarios for how the Library might use private online student information, students valued the purpose of improving the library's collection and services least of all. This resonates with Guenther's (2001) conclusion:

> As the law tries to keep pace with Internet technology, we need to protect our patrons and ourselves, to be proactive in our organizations, and to educate our patrons as best we can. A privacy statement provides a much-needed proactive measure and also re-emphasizes the role we play on behalf of our patrons- that of pathfinder and trusted agent. (p. 58)

Pace (2001, p. 50) agrees: "I am not about to advocate the creation of a union catalog of circulation activity that the FBI can tap into whenever it wants to know whether bank robbers prefer Nietzsche to Heidegger. I'm just saying that we're a little behind the curve when it comes to informing our users about privacy." Pace's statement about the lack of proactivity on the part of librarians in relation to informing users about privacy still appears to be correct: the majority of the survey respondents indicted that they were not familiar with ISU's "Code of Computer Ethics and Acceptable Use" or with the PATRIOT Act.

Libraries need a clearly defined policy for data collection, accompanied by information readily accessible to library users on how they can obtain, confirm, and challenge data that is collected about them. Users should also have the right to opt out of being included in data collection. Pace (2001, p. 51) questions whether we are educating users about our privacy policies and whether we are helping users to make educated decisions about giving up their privacy for the features in online services that our libraries license.

6. Conclusion

Many teaching faculty and librarians realize that students need to be familiar with appropriate and inappropriate use of information on the Internet. Rader (2002, p. 75) provides some strategies for teaching Internet ethics that are applicable both for information seeking as well as for gathering information based on users' transactions. Her first strategy recommends that the library be part of a campus-wide effort to develop a privacy policy that should clearly

define standards for acceptable use of transaction-based information. Ideally, the library would have a place at a campus-wide discussion that would involve many stakeholders, among those included would be the University's Administration and Legal Counsel, University Computing, and the University's law enforcement body. Rader's second strategy is to communicate ethical codes through the use of a variety of media, including disseminating print copies of a privacy policy to all stake-holders, posting it on the school Web site, and printing it in the school newspaper. If the library has a privacy policy it should be readily accessible from the library's Web site, as well as the University's Web site.

ISU students overwhelmingly value their online privacy and feel issues involving online privacy are important. ISU students are not well informed, however, about those issues or legislation and University regulations that might affect those issues. This study shows that it is important for Universities and University libraries to find a consistent method of contact with all undergraduates to inform them about privacy-related issues. Students do not usually have a clear idea of who runs what at a University. What is important is that privacy-related information maintained by the University or the library be readily accessible and proactively distributed to students. Estabrook (1996, p. 49) suggests that libraries could be proactive by asking users if they would be willing to allow the library to retain circulation data to improve service. The results of the survey also show that there would be significant interest in learning if it is possible to "opt out" of certain levels of data collection.

Bodi (1998, p. 462) provocatively writes: "Librarians and faculty continue to face the challenge of motivating students to become part of the academic community where honesty and scholarship are virtues" and her article "suggests Kant's categorical imperative, never to use another as a means but always as an end." Librarians should try to be proactive in establishing

and communicating a policy that explains to their constituency what, if any, user-transactional information is collected and if and how it is used. It is imperative that in an era of great concern over user privacy that librarians do not take advantage of users' rights, expectations, and lack of information on library-related privacy issues.

References

American Library Association. (2005). *American Library Association Code of Ethics*. Retrieved November 10, 2004 from: http://www.ala.org/ala/oif/statementspols/codeofethics/coehistory/codeofethics.pdf.

Bodi**,** S. (1998). Ethics and information technology. *The Journal of Academic Librarianship, 24,* 459-463.

Crystal, J., Geide, C., & Salpeter, J. (2000). The concerned educator's guide to safety and cyber-ethics. *Technology & Learning, 21*(4), 24–31.

Estabrook, L. (1996). Sacred trust or competitive opportunity: Using patron records. *Library Journal, 121*(2), 48-49.

Foerstel**,** H. (1991). *Surveillance in the stacks: The FBI's library awareness program*. New York: Greenwood Press.

Guenther, K. (2001). Pass the cookies and uphold the privacy. *Computers in Libraries, 21*(6), 56-58.

Hoffman, D., & Spencer, R. (2000). A Right to privacy: What students should know. *High School Magazine, 7*(8), 5-9.

Iowa State University of Science and Technology. (2004). *Code of Computer Use and Acceptable Use Policy*. Retrieved 16 May 2005from: http://policy.iastate.edu/it/ethics/

Marcella, A., & Stucki, C. (2003). *Privacy handbook: Guidelines, policy implementation, and international Issues.* Hoboken, NJ: John Wiley & Sons.

Nicholson, S., & Stanton, J. (2004). Gaining strategic advantage through bibliomining: Data mining for management decisions in corporate, special, digital, and traditional Libraries. In H. Nemati & C. Barko, (Eds.), *Organizational data mining: Leveraging enterprise data resources for optimal performance*. (pp. 247-262). Hershey, PA: Idea Group Pub.

Pace, A. (2001). It's a matter of privacy. *Computers in Libraries, 21*(6), 50-52.

Rader, M. (2002). Strategies for teaching Internet ethics. *Delta Pi Epsilon Journal 44*(2), 73-79.

Rezmierski**,** V., & Seese, M. (2002). Does information contained in systems logs at colleges and universities constitute education records? *College and University, 78*(1), 3-11.

Saftner, D., & Raghunathan, B. (1995). Privacy in the computer age. *Journal of Information Ethics, 4*(2), 43-51.

Stielow, Frederick J. (1993). The FBI and library spying: A World War II precedent. *American Libraries, 24*, 709–711.

VanScoy, A. & Oakleaf, M. (2003). *Online privacy vs. enhanced virtual reference: What do patrons really want?* Retrieved November 10, 2004 from: www.ala.org/ala/acrl/acrlevents/vanscoy.PDF.

TABLES

Table 1. Survey Response Rates for Groups

Date	Group	Students in group (#)	Students in group responding (#)	Students in group responding (%)
August 2003	fall I	148	148	100
September 2003	Honors students	158	86	54
October 2003	fall II	126	110	87
January 2004	spring I	113	100	88
	Total	545	444	81

Table 2. Familiarity with ISU Code of Computer Ethics

	fall I		Honors		fall II		spring I		TOTAL	
	No.	%	No.	%	No.	%	No.	%	No.	%
A Very familiar.	7	5	9	10	5	5	6	6	27	6
B Somewhat familiar	67	45	35	41	46	42	35	35	183	41
C Not familiar	74	50	42	49	59	54	59	59	234	53
Total	148	100	86	100	110	101	100	100	444	100

Percentages may not equal 100 due to rounding

Table 3. Student opinion of potential justifiable uses of online private information

	All Groups	
	Yes (%)	No (%)
To prevent or flush out a virus	62	38
To track down and prosecute unauthorized computer users	58	42
To manage and distribute bandwidth	25	75
To monitor web activity & content for violations of the ISU Code of Computer Ethics	38	62
To develop profiles to enhance the Library's collection and services	23	77
To aid law enforcement officials with a search warrant	58	42
There is no reason a University or Library can justifiably look at a student's private information	32	68

Table 4. Importance of online privacy

	fall I		Honors		fall II		spring I		TOTAL	
	No.	%	No.	%	No.	%	No.	%	No.	%
A Not important	6	4	4	5	4	4	4	4	18	4
B Somewhat Important	19	13	8	9	7	6	11	11	45	10
C Important	48	33	30	35	43	39	31	31	152	34
D Very important	72	49	44	51	56	51	53	53	225	51
E Undecided	3	2	0	1	0	0	1	1	4	1
Total	148	101	86	101	110	100	100	100	444	100

Percentages may not equal 100 due to rounding

Table 5. Student opinion – various aspects of online private information

	A Strongly Agree	B Agree	C Disagree	D Strongly Disagree	E Undecided
A university or library should:					
Only collect student information with informed consent	57%	35%	4%	0%	4%
Only collect student information for clearly defined purposes	49%	37%	4%	4%	6%
Never disseminate student information to outside agencies	72%	19%	5%	0%	5%
Inform students what info. is maintained about them	68%	25%	2%	1%	4%
Apply appropriated life spans to student's personal information	40%	34%	5%	2%	19%
Take responsibility for informing students about the Patriot Act	38%	40%	4%	0%	18%

Percentages may not equal 100 due to rounding