Victoria D Baker. A Content Analysis of Library Privacy Policies. A Master's Paper for the M.S. in L.S degree. May, 2013. 57 pages. Advisor: Fred Stutzman

The following study is a qualitative analysis of the content of 30 academic library privacy policies. These policies were analyzed to identify how libraries approach patron privacy through published policies. The key findings of the study include that there is a strong focus on legislation and regulatory compliance among academic libraries. Notably, there was a smaller focus on information regarding how personal records may be released and to whom they were released. Among libraries studied, there was little reference to ALA practices, policy making ethics or other guidelines. Finally, there was little emphasis on information regarding patron consent and release of information. With the advent of newer technologies and a greater population of individuals able to use and understand them, libraries must implement a variety of measures to protect patrons private records and information.

Headings:

Privacy

Libraries

Policy

Coding

Content Analysis

Legal Issues

Confidentiality

LIBRARY PRIVACY POLICIES: A CONTENT ANALYSIS

by
Victoria D Baker

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Library Science.

Chapel Hill, North Carolina

April 2013

Approved by

_____

Fred Stutzman

Contents

Introduction

This study seeks to answer one main question: W*hat trends are revealed through the analysis of library privacy policies?* In our current technological environment, new innovations are constantly being developed and used by both the government and every-day individuals. Some of these technologies are making it easier for us to interact with one another but also potentially spy on each other. This ability to view protected or sensitive documents is a trend that is of special interest to librarians. Issues with privacy are not only threatened by technology but also by new federal and local legislations such as the Patriot Act, and FERPA.

Another question that I posed during my research was the audience of the privacy policies. Would library staff or patrons derive the most benefit from a well-made policy? The American Library Association Guidelines assert that the purpose of a library privacy policy is to communicate the library's commitment to protecting users' personally identifiable information (ALA Privacy Toolkit, 1). The policy should also include 5 of the ALA's information practice principles including: notice, choice, access, security and enforcement.

Nicholson (2003) writes that in reaction to the Patriot Act, libraries were forced to develop new solutions to protect patron privacy such as daily shredding. Nicholson now suggests a less extreme measure to protect their users by transferring patron information to

a data warehouse. By removing personally identifiable information from operations systems and storing them in external warehouses, libraries are still able to evaluate transactions and other statistics. Matz (2008) similarly suggests that there lacks a "federal statute that acknowledges a right to privacy for libraries or their patron's transaction records" (Matz, 2008, p.73). Sections of FISA, a foreign intelligence act, allows for no privacy of personally identifiable histories maintained by educational establishments, including libraries. The act also allows law enforcement to view patron communications without users being aware of this invasion of privacy. The American Library Association responded by developing guidelines for reacting to FBI warrants and subpoenas. The Association encourages libraries to adopt their own policies on patron privacy, examine current policies and how they compare to the library's mission and finally to perform privacy audits to ensure patron confidentiality (ALA Privacy Toolkit, 1).

My research focused on how patron privacy could be improved within the library environment. I found that with the changes in technology and various legislations, the subject of patron privacy is not static and should consistently be revisited. One way to begin to prepare for inevitable privacy threats is by creating and implementing a well-made privacy policy. These policies would effectively serve dual purposes by protecting library users as well as the library institution.

Literature Review

1.1 Intellectual Freedoms

Librarians have been aware of the threats to their patrons' privacy and intellectual freedoms. However, a new trend that has begun to alarm libraries at the turn of the century is the potential for 3rd party vendors and governmental interference potentially threating patron privacy. Following the United States terrorist attacks in 2001 and the ability for terrorists to use library resources for harmful research purposes, the threat of governmental intrusions in libraries became more of a reality and librarians were forced to discover ways to approach these threats effectively on behalf of their patrons.

1.2 Legal Issues in Libraries

For example, in the case of Doe v Gonzales, the FBI demanded all records, digital and print, of any individuals who were logged onto a particular IP address during a certain time period (Doe v. Gonzales, 2005). Doe, the library member in question intended to inform the individuals' whose records were being accessed by the FBI, that their files were being viewed by a third- party. However the staff member contended that 18 U.S.C.S. § 2709(c), the legislation that prohibited him from revealing this information to the users of this particular IP address, was unconstitutional. The statute refers mainly to telephone or other electronic communications secured by the FBI and states that under no circumstances should these FBI requests be disclosed to the individual whom those request are directed (18 USC Sec. 2709). Doe felt that the statute restrained his right to Freedom of Speech, especially where it concerned his testimony in a hearing regarding

various revisions to the Patriot Act. Unfortunately his motion to "vacate a stay" of this law was denied.

1.3 Technology Threats to Privacy

Although the library community is apprehensive of an increase of governmental interference concerning patron privacy, they are not the only risk to patron confidentiality (Million, A. C., & Fisher, K. N. ,1986). Another factor to consider is the variety of information technologies and how those technologies are storing user information. Previously, staff were manually shredding patron records and in some cases burning them, now they are taking a less dramatic approach and are using newer and "safer" technologies to protect patron privacy. One of these new ways of protecting patron privacies is by deleting Internet cookies, "small files sent to a browser by a Web site to enable customization of individual visits" (ALA Privacy Toolkit, 2005). One example is by "hardening the browser(s)" or using a browser that has proven to be "historically secure" and configuring the settings to disable cookie retention (Kern & Phetteplace, 2012).

The interaction between the changing world of technology and library privacy is an issue that libraries need to address. There is an increase of technology used by patrons as well as that used by library staff. Online circulation systems, changing vendor policies and procedures and the advent of e-books and other e-resources, all add to the dynamic relationship between libraries and their patrons. Holstrom (1992) illustrates that patrons show less concern for how or by whom their services are given, only that those technologies are available and that they are in working order. In order to better inform

patrons of how their records are being retained and used, library policies should explicitly explain these new retention and data collection systems.

1.4 Polices and Privacy

Not only are librarians beginning to confront the risk to patron confidentiality with more reliable technologies, but also in their policies. Dixon (2008) writes that patron information stored in the authentication process should be addressed in the policy, and that disclosure allows patrons to become more aware and responsible for how their personal information, especially if it is identifiable, will be treated in a library setting. Library privacy policies should not only inform the patron that libraries may be inadvertently or purposefully storing their records via click streams or to obtain circulation statistics, but third parties such as database vendors may also have access to patron records. My study, therefore, focuses on library privacy policies. I describe many of the characteristics concerning patron privacy including: patron print and digital records, cookies, third party vendors and the legislation that affects academic library policies.

Dixon (2008) writes that FIPS or fair information practices are governmental safeguards developed to insure fair information practices are fair and provide adequate privacy protection, should also apply to the authentication process (Federal Trade Commission 2012). However, unlike many of the ALA principles relating to information confidentiality, Dixon asserts that FIPS should allow for more openness concerning patron information. New library policies would provide no privacy, assuming personal information should be readily accessible in order to better analyze circulation data.

Dixon's "openness" statement goes completely again the tenements of the American Library Association's mission statement which describes patron privacy as the library's rather than the patron's responsibility. However, as information is becoming more difficult to completely erase, there are some in the library community that believe that patrons should shoulder some of the accountability for their own privacy, which is where the need for well-made policies arise (Dixon, 2008).

Kelley, Cesca, Bresee and Cranor (2010) describe how policies could be easily formatted and understood by the general population. Although they are not members of the library community, their study on privacy policies in other environments could prove helpful to all varieties of libraries. As it now stands, library privacy policies are filled with legal jargon, are usually many pages long, and require a college level education to understand. With all of these obstacles associated with policies, many patrons do not read or care about the library's privacy policies(Kelley, Cesca, Bresee and Cranor, 2010).

Methodology

1.5 Content Analysis

In the following study, I explore the privacy policies of academic libraries and the implications of these policies for patrons. I utilized a content analysis of academic library privacy policies; this provided me with an opportunity to compile an unbiased collection of data (Neundorf 2002). The measure that is most appropriate for these policies is a manifest content analysis. A latent content analysis would inevitably require

a large amount of trained coding assistants to ensure inter-coder reliability as well as a plethora of time and resources (Babbie 2012). After deciding to use a content analysis for this research, I developed a data set for the analysis, by downloading the privacy policies of 30 academic libraries.

To do this, I first found that the Carnegie Foundation had a variety of sets containing academic institutions. Carnegie developed 3 sets that were most relevant to my research: high, very high and doctoral research data sets comprised of academic universities and colleges and transferred that data onto 3 separate Excel spreadsheets (Carnegie Foundation classification, 2012). The raw data from the Carnegie Foundation can be found on their website. I used approximately 10 universities from each of the 3 Carnegie Excel spreadsheets to develop my final 30 library privacy policies. Each of the policies was analyzed using pre-determined codes relating to legal issues, personal

privacy, third parties and library staff responsibilities. The frequency of each code was noted and further analyzed.

1.6 Classifications

The Carnegie Foundation's classifications for research institutions were used to create the random sample of final research libraries. The Carnegie Foundation compiled a list of 3 different categories. The categories were high, very high and doctoral institutions. After 2006 the Carnegie Foundation released a slightly different classification system than what they used in previous years. The new classification

system is now identified as a Basic Classification rather than Research I &II and Doctoral I & II. The Foundation writes that:

> "By providing a set of distinct classifications as well as a set of online tools for creating custom listings (combining categories within classifications, identifying institutions in similar categories across classifications, or filtering listings by selected criteria), researchers now have much greater analytic flexibility, allowing them to match classification tools to their analytic needs"(Carnegie Foundation Classification, 2012, p. 1).

Nisha Patel, the Coordinator of Carnegie's Programs and Administration division, wrote that the institutions present within each category were based on their aggregate level of research activity per-capita, according to 2008 NSF data (N. Patel, personal communication, November 27, 2012) . Unfortunately, many of the researchers responsible for comprising these various graphs and data tables were no longer employed by the time research for this project began. According to the Carnegie criteria, the doctoral granting institutions were captured and then categorized based on the aggregate level of research activity, those institutions that do not offer doctoral degrees were categorized based on the "per-capita research activity using the expenditure and staffing measures divided by the number of full-time faculty whose primary responsibilities were identified as research, instruction, or a combination of instruction, research, and public service" (Carnegie Foundation Classification, 2012, p. 1). The aggregate and per-capita indices were considered equally, such that institutions that were very high on either index were assigned to the "very high" group, while institutions that were high on at least one (but very high on neither) were assigned to the "high" group. Remaining institutions and those not represented in the NSF data collections were assigned to the "Doctoral/Research Universities" category (see appendix H).

During my content analysis of the schools, I analyzed a stratified random sample of the Carnegie Research list. This totaled approximately 30 libraries and subsequent library privacy policies. The institutions captured from the sample included public, private, liberal arts, technical, community, large, small and medium sized universities or colleges. In order to ensure that the policies would not be changed, deleted or updated during the course of this research, each policy was saved on my hard drive as a PDF file. The list of policies allowed me to refer back to the policies over the course of the project as well as provided statistical data for future research pertaining to how the policies may or may not have changed over time. After saving each policy as a PDF and noting the URL used to find the document, a quick review of the policies was needed to identify the more obvious trends in wording throughout each document. Code selection was based equally on this quick first look of the chosen policies, research literature relating to policy creation as well as my own concerns relating to libraries, patron privacy, and the importance of a clear and concise policy.

1.7 Codes

I chose particular keywords, or codes for each policy. These codes were based on what I thought were important and should be included into each document. They were also based on previous literature and other research concerning privacy policy creation. I originally planned on between 12- 15 character subheadings contained within 3 general categories. However, by the conclusion of the study 29 codes were compiled under 4 sub headings. The purpose of the subheadings were to help me in analyzing the data at the conclusion of data collection as well as providing an easier and more visual way of noting potential trends and redundancies in code words and frequencies. Due to a variety

of limitations, many of the code variations or synonyms were not captured. These similarities in wording and meaning would be an ideal start for future research.

The codes and supplementary information pertaining to the codes were compiled in an Excel Spreadsheet. The spreadsheets were contained within 3 Excel workbooks titled: high, very high and doctoral research categories. The Carnegie categorized workbook separated each policy to its own spreadsheet. This allowed me to note changes and trends both within each particular category as well as between those categories. Due to the smaller sample size, approximately 30 policies, an external data package was unnecessary. Data analysis included observing how often a code was used in each specific policy as well as an aggregate list of codes for all policies (table A).

After coding each policy in their entirety I reviewed each policy for word trends in the document. Each policy became more familiar after each subsequent review; however, the final examination of each policy would be crucial in determining trends that may have been initially overlooked in the coding process. By analyzing the language used, the length of the policy and other supplementary factors, a more comprehensive examination of each document revealed subtle similarities or differences between policies. Finally, I wanted to find examples of the best policies". The decision for the "best-practiced" policies depended on a variety of factors: how closely the policy adhered to the ALA Policy toolkit guideline, how easy the policy was to understand, the length of the policy, the amount of legal jargon or un-clear wording, how frequently the policy is updated and the presence of university contact information.

Findings/Results

1.8 Coding

Because of the large number of policies and codes, I did not code all of the policies at one time. Instead, I chose to code 5 policies a day over the course of a month. This time frame also included reviewing and observing trends in policy content. After coding each of the 30 policies, I counted those codes and made note of patterns and significant coding frequencies within each policy. The codes with the largest number of instances in all 30 of the various policies were those relating to personal and legal expectations. Both trends could be more of a recent occurrence or could have gradually evolved over the past few decades. Instead, I counted each code, noticing those that had more than 20 instances in all 30 policies. The percentage of each code was also noted by counting the total potential number of instances for all codes, 899, and dividing that number into the actual instance of the code (table A).

Understandably, due to the larger government presence and laws affecting patron privacy within libraries, legislation and the names of various laws were one of the highest codes noted. However, the codes relating to how personal records may be released and to whom they were released to were not specifically stated. Cookies, "small files sent to a browser by a Web site to enable customization of individual visits" were noted 12 times, circulation 8, subpoena 5 and court order 5 (ALA Privacy Policy Toolkit). These various codes would have been perfect opportunities for libraries to explicitly note who and for what reason a patron's private information may be released. Both the university as well as the individual patron is responsible for privacy expectations however patrons may be

unaware of their responsibilities which are further exacerbated by lengthy and jargon-filled policies. With those concerns in mind, there were also smaller emphasis placed on those codes relating to patron consent and release (appendix D).

Similar to the small number of court related codes, vendors and other third parties were mentioned 4 times in all 30 policies. One explanation could be an increase in external resources in libraries due to new trends in technology and other academic resources, those vendors and other external industries do inevitably use private patron information. And because these vendors are separate from the library, patrons would fall under the purview of the third-party's policies. The literature suggests that this oversight in policy wordage may not be deliberate. Many library staff are unaware that when a patron uses an external database or other resources that they are effectively agreeing to the policies of those vendors. By better educating library staff these oversights would not be missed.

Similarly, a portion of the policies did not have visible contact information. Approximately half of the university libraries gave patrons the opportunity to ask questions or give comments on the privacy policies. Finally, there were less code instances referring to ALA practices, policy making ethics or other guidelines. Although this small number of codes does not necessarily mean that the policy did not utilize ALA resources, it would reassure users that the document followed an authoritative set of guidelines and standards. The ALA toolkit and examples, though lengthy, describe in detail the components of a well-written library privacy policy. They also outline what are known as the five "Fair Information Practice Principles" (Federal Trade Commission,

2012). The principles described below include the rights of notice and openness, choice, access, security and enforcement.

1.9 ALA Principles

The American Library Association defines the right of notice and openness as a patrons' rights to both privacy and confidentiality and how their personal information may be potentially used in the library setting. Patrons should also be aware of what "personally identifiable information (PII) is gathered about them, where and how it is stored (and for how long), who has access to that information and under what conditions, and how PII is used" (ALA Privacy Toolkit, 1). Choice and consent is similarly described as fully explaining how patrons' personal information may be collected and used by library staff. Access by users allows patrons the rights to their own personally identifiable information and gives libraries the responsibility of ensuring that the devices that store PII function properly. Data integrity and security also hold libraries accountable for "taking reasonable steps to ensure integrity, including using only reputable sources of data, providing library users access to their personal data, updating information regularly, destroying untimely data or converting it to an anonymous form, and stripping PII from aggregated, summary data" (ALA Tool Kit, 1). The ALA Tool Kit goes on to define the various forms of library security that patrons should expect concerning their private information which includes electronic tracking and various administrative measures. The fifth and final principle includes enforcement and redress which describes the need for well-made policies, audits and the capabilities and resources to enforce both. I attempted to find mirrored in many of my chosen privacy policies,

these clearly defined principles. Because the ALA has provided the tools for developing a comprehensive and informative privacy policy, I felt that many of the policies should have included, referenced or reflected these ideals.

1.10 Categories

Because of the large number of codes, I needed to categorize each of the codes so that I would be better able to notice trends and ultimately keep my data separated and relatively easy to analyze. Each of the categories contained codes that were related to one another in some way. For example the category “internal uses” referred to patron data being used by library staff, so “circulation” and “administration” were included in that category (table B). By grouping the codes into categories, I was also able to code more efficiently especially if the policy was separated into similar labeled sections. Luckily, many of the policies were broken up in this way which made my coding process faster.

The general categories were internal uses, legal expectations, personal expectations and third party responsibility. For example: code third party would refer to external organizations whose products are used in the library environment, a subcategory is vendors. Many libraries do not view library vendors’ privacy policies as affecting their own policies (Magi 2010). Both the codes as well as the words surrounding the code were copied into the Excel spreadsheet. For each category the frequency of the factor, notes and context of the quotes as well as the type and size of the school were noted. This allowed for a better comparison of each policy and for this research to be replicated. The frequency of each updated policy was also noted as well, the length of the policy in page numbers and finally any final thoughts, comments or remarks on the policy. For example

the researcher may have described how difficult or easy the policy was to find on the library's main page. Perhaps if the policy was not easily found it may or may not also be assumed that it is not updated regularly or may not be comprehensive.

Discussion

I found a variety of troubling issues in many of the policies. Some were not updated, or were updated irregularly, others switched between third and first person making the policy difficult to read and understand and still others were filled with legal jargon. Another varying characteristic in each of the policies were their length. Although some research suggest that longer policies may provide more comprehensive information, if those lengthier policies are filled with difficult terminology and definitions, then patrons may not read the entire policy and it would ultimately not serve its informative purpose.

Million and Fisher (1986) write that it would be detrimental to both libraries and patrons to develop a policy that no one would ultimately peruse. They write that policies have become more important over the years because of the advent of state and federal laws and regulations that affect libraries and their users. In 1986, when the Million and Fisher published their article concerning library records, 18 states had laws that concerned library records, revealing that libraries would need to be aware of these confidentiality laws and regulations and echo those concerns in their policies. One example of a larger legal influence in libraries is the libraries' inability to notify a patron of a potential court order while also forcing library staff members to release a particular patron's information. Jones (2010) writes that there are also global implications for

protecting the intellectual freedoms of patrons and that it is the library's responsibility to understand federal and local laws that can be applied to library patrons. Bennet (1997) similarly writes that privacy policies in Canada need less fragmented standards for protecting personal information.

Reutty (2007) writes in "*What happened to me when the police came knocking*…" that in 2007 police confronted the library director about releasing a particular patron's records. The author states that this event resulted in specific library policies on how to respond to police interference in the library. Fault (2004) similarly states that policies are important to guide library personnel behavior. Both legal and administrative concerns should be addressed in privacy policies especially those relating to library user personal information.

Similarly, data concerns should also be described in policies in greater detail. Sutlieff and Chelin (2010) describe that libraries are aware of privacy concerns but are not prepared to deal with data protection. The authors state that more explicit policies should inform both patrons and staff that their information may be viewed and used by library administration or an external third party.

1.11 3 Case studies for "best use" policies

1.12 Policy Characteristics

In the following section I will introduce 3 of the "best practiced" policies. The criteria for each of the three "best practiced" policies included a number of elements. The length of the policy, described by Voeller (2007) should not be too short.

Policy Characteristics
1. Length a. Not too long or too short
2. ALA References/Standards a. Based on Tookit and Code of Ethics
3. Vendor Accessibilities
4. Patron Computer Conduct
5. Staff Access to Patron Records
6. References to Parent Institution
7. Well Publicized a. Digitally and Physically

A short policy is described as having little to no effort put into its creation. Voeller (2007) also describes that the more authoritative policies should be based on ALA standards especially those in the library bill of rights and the library code of ethics. With that in mind, I also noted if the three best practiced policies included a reference to ALA organization as well as the ALA privacy guidelines. Burkell and Carey (2011) similarly wrote that those policies that are based on the American Library Association's privacy toolkit should also be implemented in libraries overseas. They write that Canadian libraries are also aware of patron privacy issues, however many smaller libraries lack the resources or authority to enforce those policies. The authors describe that many of the principles of patron privacy protection include notice, choice, awareness, integrity and enforcement and that due to the Patriot Act and the subsequent concerns for patron privacy, many Canadian libraries have begun to adopt privacy policies.

I used Vaughan's (2007) study on record retention policy construction at the University of Nevada Las Vegas to develop the 3 best practiced policies (appendix j,l,n). The UNLV library studied their own record retention and developed step-by-step instructions on how they developed their library policy. During this process UNLV consulted local libraries, ALA review, Federal Law review, and spoke with various IT systems experts on the viability of a data retention policy. Similarly, other factors that

affect policy construction procedures are digital reference and librarian-patron confidentiality. Library vendors do in most cases, have complete access and control over electronic chat records. Compounded to 3rd party access capabilities are the ambiguity of laws and the lack of federal statutes protecting library patron's privacy.

However, Neuhaus (2003) describes that there are other avenues to protecting patron privacy. Some of those solutions include limiting the amount of information discussed in chat reference sessions to only that needed for the transaction, severing personally identifiable tags, and finally allowing only upper level personnel access to patron records. Neuhaus (2003) also gives helpful advice for developing and advertising a library's privacy policy. He writes that the document should be prominent both in the physical and digital library space, it should address ethical issues concerning privacy and conform to both the ALA code of ethics and the institutions general privacy policy. Carter goes on to specify how privacy policies should also explicitly address privacy and technology.

In the case of both public and private academic libraries, computers are publicly accessible to students, faculty, staff and in some cases, alumni. Passwords for computers should be erased after a set period and misuses under a specific password should be addressed with disciplinary actions. The policy must also reflect the ideals and values of the community by referencing particular laws and university honor codes or policies.

Although each of these researchers described varying characteristics that should be included in the "best" library privacy policies, there were similarities between the authors' suggestions. ALA references, community awareness including references to the parent institution as well as local and federal laws, and finally information concerning

vendors' policies and when a patron would fall under this 3rd party's purview were all themes echoed with researchers. As I began to develop the 3 "best practice" policies these elements, as well as other personal policy preferences were used.

One of each of the three policies were chosen from each of the Carnegie Foundation's three academic categories: high, very high and doctoral institutions. I specifically searched for policies that were not excessively long, that did not contain a plethora of legal jargon and were relatively balanced in each of my 4 coded categories: internal use, legal expectations, personal expectation and third party. I was also looking at how the policy was sub-divided, if the definitions were relatively easy to understand and finally if there was available contact information.

1.13 Illinois State University

Illinois State University, an institution in the doctoral research institutions category, was the first chosen of the best practiced privacy policies (appendix I). The document was of medium length, a bit over 4 pages. The language was easy to understand, and the policy was introduced and described effectively in the first paragraph. The introductory paragraph referenced the ALA and the Library Records Confidentiality Act. Key terms were also bolded and described with a minimum of legal jargon or confusing language. There were also multiple links within the document that would provide the user with more detailed descriptions of various terms within the document. Cookies and third parties were also described within the policy. Also if the user had more questions or concerns, the contact information for Dane War, the Interim Dean of University Libraries, was provided as well as a working link to his photograph

and other contact information. Finally, the policy was reviewed by the Illinois State University's Office of General Counsel a year prior to the start to this study, and was explicitly stated at the end of the document. One improvement that could be made to the policy would be an increase of white space. Because of the length of the document, partially due to the large amount of links and definitions, the white space may have been removed to conserve space. However, it worked conversely and made the policy appear cluttered and lengthy.

1.14 George Washington University

The next policy I chose was George Washington University, a member of the very high research institution category (appendix m). It contained similar characteristics to Illinois State University's privacy policy. This document was relatively short, 3 pages, and contained a large amount of white space. Each subheading was described in a way that was easy to understand. Unfortunately, the date of the last revision was not supplied and the policy informed users that the document may be updated without notice. The policy also informed users that Google Analytics may be used to "collect certain information automatically upon a user's visit (George Washington University Privacy Policy)." The document also stated that numerous other University policies may relate to this one. The policy did contain University contact information however it was limited to an email address with no accompanying name.

1.15 University of Alabama

The University of Alabama's academic library, an institution in the high research category was the final policy I selected (appendix k). This policy was the shortest in page length, out of the three. The document was a bit text heavy and although it was divided into separate paragraphs, those paragraphs were not delineated with keywords describing their content. One of the most appealing elements to the policy were the active links at the top of the page directing patrons to the university's copyright statement, policies,

contact information and other helpful information. The policy did contain information on third party expectations, laws and cookies. I chose this page mainly due to its length, functional links and the lack of legal jargon.

Limitations

There were a number of limitations within this project. Because there was one person coding, re-coding and analyzing the data, a smaller n-value was necessary in order for the research to be completed in a timely fashion. Also due to the time constraints much of the data was not as robust as they could potentially have been. All of the universities varied in size and type however due to the smaller sample size and the risk of forming false positives, much of that data was not analyzed.

The coding process was similarly affected by my time constraints. Many synonyms were not coded, and those may have significantly affected the results. Although there were necessary and unavoidable time restrictions, I did attempt to use some, but not all variations on words. For instance various tenses were captured which may have inadvertently biased results but also may have acted as a counterbalance to the

missing coded synonyms. Finally, the very nature of the methodology used was a substantial limitation. I decided on a manifest rather than content analysis in order to circumvent the need for multiple coders and resources as well as high inter-coder reliability.

Future Directions

Although there were obvious limitations to the study, many of those restrictions could be used to positively direct future researchers. A larger sample size and greater granularity of university types and sizes would be a start for prospective research on the topic of library privacy policies. As well as heavier emphasis on patron and staff surveys on the wording and policy usability. Perhaps focus groups along with surveys and naturalistic observations could aid librarians and other university professionals in developing and implementing privacy policies not only in libraries but within the university environment as a whole. By analyzing information retrieved from an assortment of institutions: large, small, community, technical, liberal etc., university and library officials would be better able to customize and fit their policies for their specific institutions.

Researchers have begun to develop and implement more user-friendly policies. Angulo et al (2012) described these innovative privacy policy interfaces as transparent and understandable by effectively allowing staff to decide how much information should be revealed. More visual and less textual representations of policies are being tested and

encouraged in order to decrease the overwhelming feeling that a large amount of text would incur. Finally, a rather interesting approach has been developed by the Cylab Usable Privacy and Security Laboratory (2010), describing policy development and appearance similar to that of a nutrition label. In fact, it is referred to as a "privacy nutrition label." The policy would be easier to understand for both patrons and staff. Kelley et al (2010) implemented a study on the usability and understandability of current privacy policies. She found that few read the policies because they required a college level education to understand and even then many described policy reading as "torture" however this new nutrition label based approach makes understanding and agreeing to the various facets of a policy much easier to understand (appendix g).

Conclusion

Although, there are numerous threats to patron privacy, policies may be the first step in providing users with more protection while using library materials and resources. The first step in developing better policies is to consult with an authoritative entity in the library environment. The American Library Association is not only an authoritative figure in the library profession but it also provides tools and other resources for developing well-made policies. During my research, I found that many of the policies did have errors and issues that should be better addressed. However, I also found that there are researchers both within and outside the library community that are actively searching for ways to make policy development and implementation easier. Librarians have always

been concerned with patron privacy; however that privacy has been threatened in a variety of ways and they must continue flex and adjust to these new threats. Whether it is a higher governmental influence or the risk of harmful technologies, with the help of individuals and organizations also concerned with patron privacy and confidentiality, libraries may be able proactively protect their users.

Table A

At least 1 instance of each code per policy

Codes	Instances(raw number) /percentage out of total number of instances (899)	Code Meanings/Reasoning
1. Administrative	13/1.4%	Who will be looking at personal info
2. circulation	8/.88%	Reason for looking at personal info
3. web	21/2.3%	When info will be retrieved
4. We	12/1.3%	Responsibility of university to retrieve info/who will be looking at it (1st person means more personally responsible)
5. cookies	12/1.3%	When info could be retrieved
6. records	18/2.0%	What personal info is called
7. retention	8/.88%	Schedule of docs kept for analyzing

8. Acts	17/1.8%	Why rec may be given out
9. legislation (names)/law	33/3.6%	Why rec may be given out
10. court order	5/.55%	Why rec may be given out
11. subpoena	5/.55%	Why rec may be given out
12. expectation	1/.11%	Patron should expect certain sort of privacy when using library equipment
13. personal/ confidential	44/4.8%	Sensitive information
14. private	26/2.8%	Sensitive information
15. identification	18/2.0%	Whose sensitive information
16. release	4/.44%	Patron responsibility to be knowledgeable of information given to library
17. permission	6/.66%	Patron responsibility to be knowledgeable of information given to library
18. consent	9/1.00%	Patron responsibility to be knowledgeable of information given to library

19. misuse	6/.66%	If patron misuse property in anyway, university has authority to bar patron from lib/university
20. responsibility	15/1.6%	Accountability of patron information/who is belongs to
21. questions	15/1.6%	University Information for comment/questions
22. contact	10/1.1%	University Information for comment/questions
23. parent institution	1/.11%	Reminder of institution responsibilities
24. university	20/2.2%	Reminder of institution responsibilities/more personal
25. vendors	4/.44%	Patron rec falls under 3rd party when using vendor resources
26. third party	14/1.5%	Patron rec falls under 3rd party when using vendor resources
27. ALA references	5/.55%	Commitment to follow standards of professional organization
28. purpose	18/2.0%	University purpose/missino coincides

		or not with libr policy (may be same)
29. mission	4/.44%	University mission/purpose coincides or not with libr policy (may be same)

Colored Sections:

Internal Use

Legal Expectations

Personal Expectations

Third Party

Table B

Internal Use

Codes	Instances(raw number) /percentage out of total number of instances (899)	Code Meanings/Reasoning
1. Administrative	13/1.4%	Who will be looking at personal info
2. circulation	8/.88%	Reason for looking at personal info
3. web	21/2.3%	When info will be retrieved
4. We	12/1.3%	Responsibility of university to retrieve info/who will be looking at it (1st person means more personally responsible)
5. cookies	12/1.3%	When info could be retrieved

Table C

Legal Expectations

Codes	Instances(raw number) /percentage out of total number of instances (899)	Code Meanings/Reasoning
1. records	18/2.0%	What personal info is called
2. retention	8/.88%	Schedule of docs kept for analyzing
3. Acts	17/1.8%	Why rec may be given out
4. legislation (names)/law	33/3.6%	Why rec may be given out
5. court order	5/.55%	Why rec may be given out

Table D

Personal Expectations

Codes	Instances(raw number) /percentage out of total number of instances (899)	Code Meanings/Reasoning
1. personal/ confidential	44/4.8%	Sensitive information
2. private	26/2.8%	Sensitive information
3. identification	18/2.0%	Whose sensitive information
4. release	4/.44%	Patron responsibility to be knowledgeable of information given to library
5. permission	6/.66%	Patron responsibility to be knowledgeable of information given to library
6. consent	9/1.00%	Patron responsibility to be knowledgeable of information given to library
7. misuse	6/.66%	If patron misuse property in anyway, university has authority to bar patron from lib/university
8. responsibility	15/1.6%	Accountability of patron information/who

		is belongs to
9. questions	15/1.6%	University Information for comment/questions
10. contact	10/1.1%	University Information for comment/questions

Table E

Third Party

Codes	Instances(raw number) /percentage out of total number of instances (899)	Code Meanings/Reasoning
1. parent institution	1/.11%	Reminder of institution responsibilities
2. university	20/2.2%	Reminder of institution responsibilities/more personal
3. vendors	4/.44%	Patron rec falls under 3rd party when using vendor resources
4. third party	14/1.5%	Patron rec falls under 3rd party when using vendor resources
5. ALA references	5/.55%	Commitment to follow standards of professional organization
6. purpose	18/2.0%	University purpose/missino coincides or not with libr policy (may be same)
7. mission	4/.44%	University mission/purpose coincides or not with libr policy (may be same)

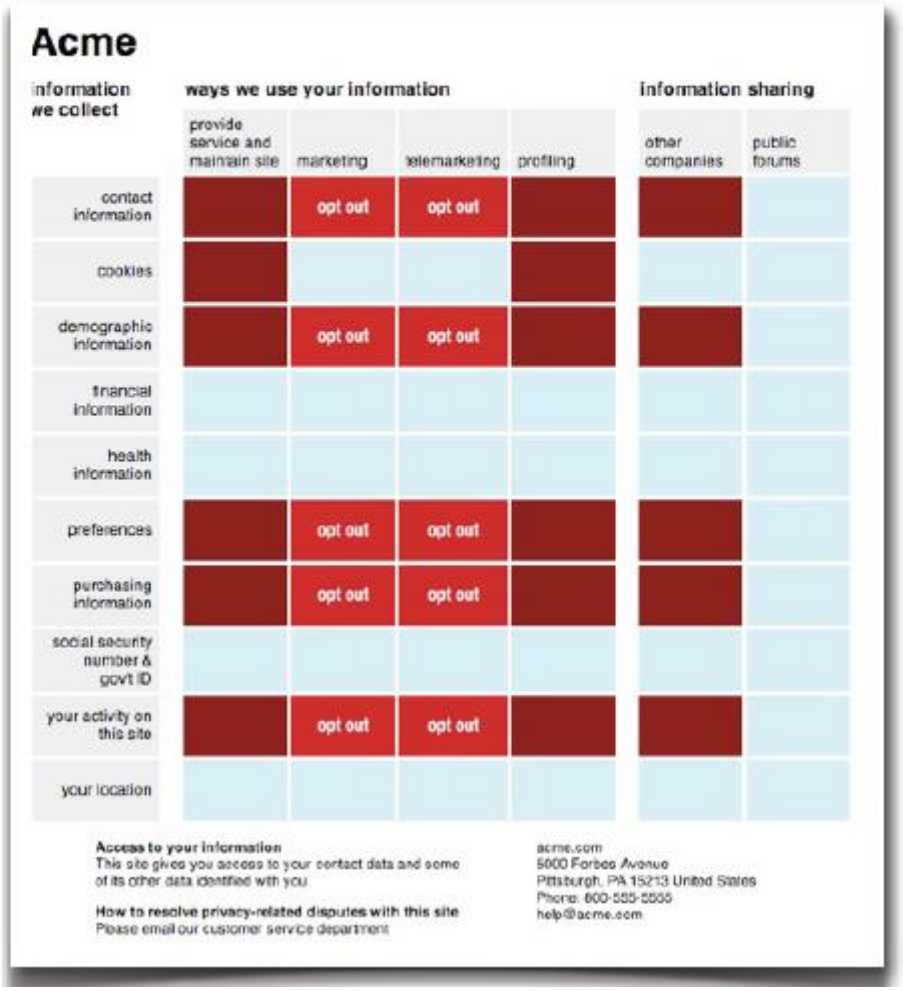
Table F

Aggregate Table

5 or more instances of 1 code	10 or more instances of 1 code	10 or more instances of 2 codes	10 or more instances of 3 codes	10 or more instances of 7 codes	10 or more instances of 8codes
58	5	3	5	1	1

Appendix G

Standardized Label



Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt out	opt out	■	■	
cookies	■			■		
demographic information	■	opt out	opt out	■	■	
financial information						
health information						
preferences	■	opt out	opt out	■	■	
purchasing information	■	opt out	opt out	■	■	
social security number & govt ID						
your activity on this site	■	opt out	opt out	■	■	
your location						

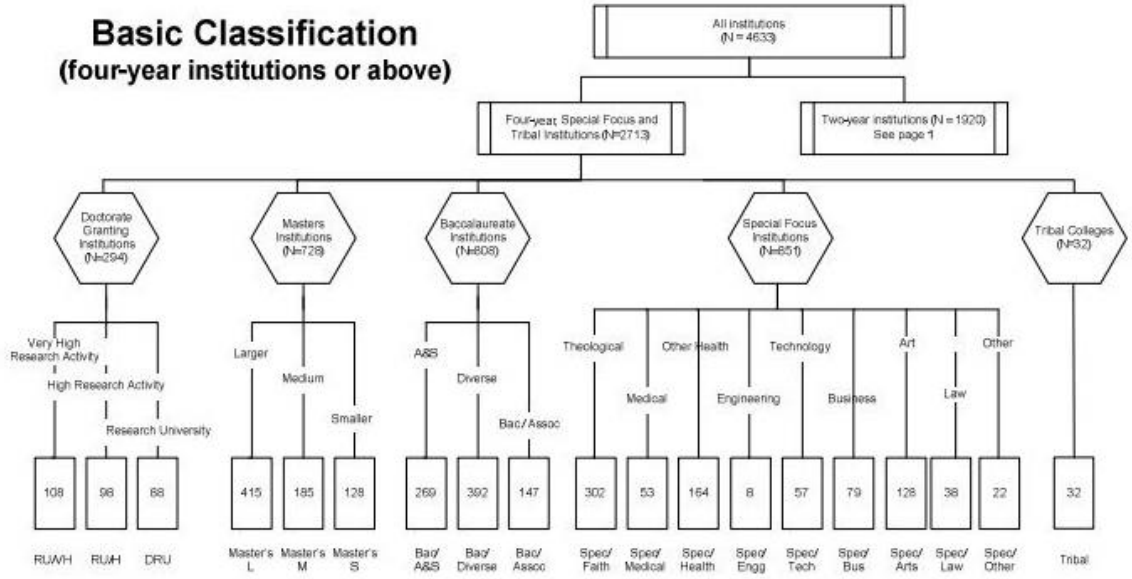
Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Appendix H

8



Notes: These flowcharts represent the logic of each of the six all-inclusive classifications. The numbers in the boxes indicate how many institutions are in that category. These numbers are approximate. Special focus institutions are only included in the Basic and Enrollment Profile Classifications. For detailed information regarding the classification methodology, please see the Methodology section on the Classification website.

Appendix I

Privacy Policy
Illinois State University, Milner Library

Illinois State University's Milner Library ("the Library", "we", "us", "our") respects your privacy. We have developed this privacy statement to inform you what information we collect, how we use, protect and release it, and how you are entitled to access it. This privacy statement applies to the web sites we administer, the email you send us and electronic services we provide.

Milner Library is committed to the American Library Association'sLibrary Bill of Rights. We adhere to the State of Illinois' Library Records Confidentiality Act (75 ILCS 70).

When you visit our web sites to read or download information, we do not collect personal information about you. In particular, we do not use "cookies" to collect or store personal information. We do use personal information that you supply in online forms, email, and other requests for information and services to respond to your requests. This may involve redirecting your inquiry or comment to another person or department better suited to meeting your needs.

Information that the Milner Library may gather and retain about current and valid library users includes, but is not limited to, the following:

□ **Circulation Information**: Patron records contain patrons' names, home addresses, telephone numbers and e-mail addresses supplied to us by the Registrar and by Human Resources. Records are purged within three years of the patron's last date of university employment or enrollment. Milner Library maintains records of circulation transactions only until the borrowed item is returned to the library or outstanding fines are paid. The library does not maintain patron histories of previously borrowed items or paid fines.

□ **Collection Development**: This includes information regarding the request, purchase, transfer, and related collection management requests linked to individual users or groups of users (e.g., departments).

□ **Computer Workstation Usage**: Patrons using computers in Milner Library must follow the ISU Policy on Appropriate Use of Information Technology Resources and Systems (ISU Policy 9.2) and theMilner Library Computer and Internet Acceptable Use Policy. Event logs are saved on individual computers; these logs are deleted whenever computers are rebuilt. Login information is gathered and stored by a campus system.

Guest patrons are required to sign in with photo identification, as requested by the Campus Police and Telecommunications & Networking, and sign-in sheets are kept at the reference desk and are shredded every 30 days.

☐ **Electronic Access Information**: This includes all information that identifies a user as accessing specific electronic resources, whether library subscription resources, electronic course reserves, or other Web resources. Milner Library utilizes web sites and subscription database that may be governed by their own privacy policy. Milner Library website contains links to websites and licensed database that are not maintained or supported by ISU. In some cases, library services may be provided via third party tools. While you may reach these services via Library web sites, you are subject to the privacy policy of third parties, and the Library encourages users of these services to be aware of their policies before using them.

☐ **Interlibrary Loan / Document Delivery**: This includes all information that identifies a user as requesting specific materials.

☐ **Library Surveys / Assessment Projects**: This includes any information or data obtained through surveys (group or individual interviews or other means) in support of assessment of services, collections, facilities, resources, etc., or in support of research related to library and information services. Any data collected in the course of research is subject to additional review of privacy and confidentiality protections (ISU's Research and Sponsored Program's *Research Ethics and Compliance*).

☐ **Reference/Research Consultations**: When contacted by a patron for reference or research assistance, we typically ask patrons for their name, contact information, nature of their query, and resources already consulted by the patron. We use this information to respond to the patron as effectively and efficiently as possible. We maintain the following information about each reference or research transaction: date, time, type of inquiry, method used by the patron to contact the library, patron status (e.g., student, faculty, and community member), the question, and our response. Until purged, patron information is available for review only by our reference faculty and staff.

□ **Rare Books, Special Collections and Archives**: Patrons are asked to complete a patron registration form that asks for name, contact information, status, institutional affiliation and research interests/purpose. These forms are shredded at the end of academic year.

□ **User Registration Information**: This includes any information the library requires users (faculty, staff, students, or others) to provide in order to become eligible to access or borrow materials. Such information includes addresses, telephone numbers, and identification numbers.

□ **Web Site**: As part of the campus network, Milner Library utilizes Google Analytics. For more information, please refer to the Google Analytic's site and Google's privacy policy page.

□ **Other Information Required to Provide Library Services**: This includes any identifying information obtained to provide library services not previously listed.

Data Integrity and Security

The data we collect and maintain at the library must be accurate and secure. Although no method can guarantee the complete security of data, we take steps to protect the privacy and accuracy of user data. The ISU Library is committed to investing in appropriate technology to protect the security of personally identifiable information while it is in the library's custody. We also pledge to work with third-party information service suppliers who have similar respect for protecting personally identifiable information.

□ **Services that Require User Login**: In-library computers allow use of most library resources without logging in. Use of the full resources of the World Wide Web and of the full power of some subscription databases requires that a user log on to the workstation, either with his/her ULID and password or with a guest account. Data about which users were connected to which machine is collected, in accordance with University policy, and stored with very limited access by staff. Users of electronic resources that require authorization for their use are also asked to log in when they connect from outside the university IP address ranges. The data kept from these transactions does not include information linking the user to the resources to which the user connected or about searches completed and records viewed.

□ **Cookies**: Cookies are used to store session information. These cookies are session cookies and are removed when the user exits the catalog and closes the browser. The library catalog and some licensed databases also use cookies to remember information and provide services while the user is online. Users must have cookies enabled to use these resources. Users of Milner computers can disable cookies during their usage. Cookies, web

history and cached files are removed when a user closes a browser or logs off a machine.

□ **Security Measures**: Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and prohibit those individuals with access from utilizing the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

□ **Staff Access to Personal Data**: We permit only authorized Library staff with assigned confidential passwords to access personal data stored in the Library's computer system for the purpose of performing library work. Milner Library will not disclose any personal data collected from users to any other party except where required by law, to report a suspected violation of law or University policy, or to fulfill an individual user's service request. We do not sell or lease users' personal information to commercial enterprises, organizations or individuals.

Relevant Links

□ American Library Association's *Library Bill of Rights*

□ *Family Educational Rights and Privacy Act (FERPA)*

□ Illinois State University's *Freedom of Information Act Implementation Rules* (ISU Policy 7.1.5)

□ Illinois State University's *Policy on Appropriate Use of Information Technology Resources and Systems* (ISU Policy 9.2)

□ Illinois State University's *Web Privacy Notice and Practices*

□ *Milner Library Computer and Internet Acceptable Use Policy*

□ State of Illinois' *Library Records Confidentiality Act*(75 ILCS 70)

□ United States Department of Justice's *USA PATRIOT Act*

Questions

If you have questions regarding this policy, please contactDane Ward, Interim Dean of University Libraries.
Adopted 7/29/11 (It will be reviewed again at the beginning of each fiscal year) Reviewed 8/18/11 by Illinois State University's Office of General Counsel

Illinois State University's Milner Library received permission from the IUPUI University Library,

Texas A&M and University of Chicago Library to adapt their patron privacy policies.

Appendix J

Patron Privacy Policy
Illinois State University, Milner Library

Illinois State University's Milner Library ("the Library", "we", "us", "our") respects your privacy. We have developed this privacy statement to inform you what information we collect, how we use, protect and release it, and how you are entitled to access it. This privacy statement applies to the web sites we administer, the email you send us and electronic services we provide.

Milner Library is committed to the American Library Association's Library Bill of Rights. We adhere to the State of Illinois' Library Records Confidentiality Act (75 ILCS 70).

When you visit our web sites to read or download information, we do not collect personal information about you. In particular, we do not use "cookies" to collect or store personal information. We do use personal information that you supply in online forms, email, and other requests for information and services to respond to your requests. This may involve redirecting your inquiry or comment to another person or department better suited to meeting your needs.

Information that the Milner Library may gather and retain about current and valid library users includes, but is not limited to, the following:

- **Circulation Information:** Patron records contain patrons' names, home addresses, telephone numbers and e-mail addresses supplied to us by the Registrar and by Human Resources. Records are purged within three years of the patron's last date of university employment or enrollment. Milner Library maintains records of circulation transactions only until the borrowed item is returned to the library or outstanding fines are paid. The library does not maintain patron histories of previously borrowed items or paid fines.
- **Collection Development:** This includes information regarding the request, purchase, transfer, and related collection management requests linked to individual users or groups of users (e.g., departments).
- **Computer Workstation Usage:** Patrons using computers in Milner Library must follow the ISU Policy on Appropriate Use of Information Technology Resources and Systems (ISU Policy 9.2) and the Milner Library Computer and Internet Acceptable Use Policy. Event logs are saved on individual computers; these logs are deleted whenever computers are rebuilt. Login information is gathered and stored by a campus system.

Appendix K

Privacy Statement

□ Copyright Statement

□ Disclaimer

□ About This Site

□ Policies

□ Contact UA

The University of Alabama respects your privacy and collects no personally identifiable information about you unless you affirmatively choose to make such information available to us. The University does not actively share personal information about Web site visitors. Personal information provided by visitors, such as e-mail addresses or information submitted via online forms, is used by the University to assist individual visitors as necessary. This assistance may involve redirecting an inquiry or comment to another University individual or unit better suited to provide resolution.

The University analyzes its Web server log files to collect summary information about visitors to its Web site. The University also subscribes to Google Analytics, which uses cookies to collect anonymous traffic data. This information is analyzed by UA and by Google Analytics to generate summary statistics for purposes such as guiding design considerations, determining successful site segments, and determining problem areas. However, because The University of Alabama is a public institution, some information collected from The University of Alabama's Web site may be subject to the Alabama Open Records Act, or in some instances the University may be compelled by law to release information gathered from University of Alabama Web servers. Some Web servers at The University of Alabama may adopt different privacy statements as their specific needs require that differ from this statement.

The University of Alabama is a research institution. At anytime there are numerous online surveys being conducted on the University of Alabama Web site. Confidential information gathered in these online surveys is used only for the research purpose indicated in the survey. Unless otherwise noted on the specified survey, your answers are confidential and individual responses will not be shared with other parties unless required by law. Aggregate data from surveys may be shared with external third parties.

The University of Alabama also complies with the Family Educational Rights and Privacy Act ("FERPA"), which prohibits the release of educational records without student permission. For more details on FERPA, currently enrolled students should consult the

University of Alabama Student Handbook or the University's Office of Academic Records and University Registrar.

Please direct any questions about this privacy statement, the practices of any University of Alabama Web site, or your use of this Web site to the Office of Web Communications.

Appendix L

Privacy Statement

- Copyright Statement
- Disclaimer
- About This Site
- Policies
- Contact UA

The University of Alabama respects your privacy and collects no personally identifiable information about you unless you affirmatively choose to make such information available to us. The University does not actively share personal information about Web site visitors. Personal information provided by visitors, such as e-mail addresses or information submitted via online forms, is used by the University to assist individual visitors as necessary. This assistance may involve redirecting an inquiry or comment to another University individual or unit better suited to provide resolution.

The University analyzes its Web server log files to collect summary information about visitors to its Web site. The University also subscribes to Google Analytics, which uses cookies to collect anonymous traffic data. This information is analyzed by UA and by Google Analytics to generate summary statistics for purposes such as guiding design considerations, determining successful site segments, and determining problem areas. However, because The University of Alabama is a public institution, some information collected from The University of Alabama's Web site may be subject to the Alabama Open Records Act, or in some instances the University may be compelled by law to release information gathered from University of Alabama Web servers. Some Web servers at The University of Alabama may adopt different privacy statements as their specific needs require that differ from this statement.

Appendix M

Privacy Policy

The George Washington University is committed to respecting users of GW's websites. For that purpose, this policy has been adopted to address the collection and use of information from GW's websites. In order to maintain effective privacy practices, GW retains the right to update this policy without notice.

Information Gathering

GW collects two types of information from users: (1) Information provided by the user in order to receive requested information and/or services, and (2) Information passively collected upon a user's visit to GW's websites.

Passively Collected Information

When a user visits one of GW's websites, some information such as the visitor's Internet protocol (IP) address, Internet service provider, operating system, the site from which the visitor arrived, and the time and date of the user's visit may be collected automatically as part of the software operation of the website. This intake of information is not personally identifiable. GW uses this information solely for internal purposes, such as, to see what pages are most frequently visited, in order to improve the site. Additionally, GW is currently using Google Analytics, a web metrics service, to collect certain information automatically upon a user's visit. For more information regarding Google Analytics, see Google's privacy policy.

Information Provided by the User

Users may provide GW with non-personally and personally identifiable information in order to utilize certain services and retrieve information. Such instances may not be noticeable to the user and include, but are not limited to: filling out surveys, purchasing goods and services, submitting tests, registering for courses, and submitting certain online forms.

Should the user choose to provide GW with any personal information, GW will use such information only to conduct official University business and will disclose it only when such disclosure may be appropriate to comply with applicable law, to enforce GW's Visitor Agreement, or to protect the rights, property or the safety of visitors to GW's websites, the University community or the public. GW does not sell, trade, or rent users' personal information to others.

GW maintains information collection procedures that comply with The Child Online Privacy Protection Act of 1998. If you believe that GW has collected personally identifiable information about your child, please contact GW immediately at comply@gwu.eduso that if such information has been collected, GW may take appropriate action.

Distribution of Collected Information

In certain instances, in order to provide information and services, or as required by law, GW may disseminate non-personally and personally identifiable information to third parties and officials/departments within GW. In these instances, the information provided to the third-party or GW entity shall be limited to the extent necessary required to provide the user-requested information and/or services, or as required by applicable law enforcement agencies.

Cookies

GW's websites make use of "cookies," which are small text files placed on the user's computer to keep track of information about the user's browsing on this site. The utilization of cookies allows GW to enhance a user's experience by allowing GW to create tailored web applications. A user's decision to set his or her web browser to accept or disable cookies is a personal choice. However, some of GW's websites may not function properly if cookies are disabled.

Third Party Websites and Content

GW websites may contain links to other websites owned by third parties as a convenience to the user. If a user decides to use these links, he or she will leave the GW website. GW is not responsible for the privacy practices or the content of such websites, and does not make any representations or endorsements about them. If a user decides to leave the website and access any third party site, it will be at the user's own risk, and users should be aware that GW's policies will no longer govern. Users should review the applicable terms and policies, including privacy and data gathering practices, of any site to which the user navigates away from GW's websites.

The User's Personal Account

Any user that chooses to use GW's websites is responsible for maintaining the confidentiality of his or her account and password, if any, and for restricting access to his or her computer, and agrees to accept responsibility for all activities that occur under his or her account or password. The user agrees that any billing and registration information provided on the websites will be accurate and complete.

Security

GW implements stringent security measures to promote the confidentiality, integrity, and availability of any information in the possession (or control) of GW. GW utilizes Secure-Sockets Layer (SSL) encryption technology for instances where GW websites request or provide personal information of the user. The SSL technology's purpose is to protect users' information from being viewed by an outside third-party.

Some features on this website may enable credit card transactions in order for users to purchase a variety of goods and services. Credit card transactions are completely voluntary. GW's security measures comply with PCI Data Security Standards (DSS). Additionally, GW exports the processing of online transactions to PCI DSS certified institutions to further promote effective security.

While the security of users' personal information is of the utmost importance to GW, GW cannot guarantee the security of any information the user chooses to disclose online. Any information the user chooses to disclose to GW is done at his or her own risk.

Policies

Below are a number of pertinent policies and procedures implemented by GW related to this policy:

- The George Washington University Privacy Policy Statement

- Data Classification Security Policy
- GW Web Content Policy
- Security Breaches Involving Confidential Personal Information
- Information Security Policy
- Health Information Privacy Policy
- Privacy of Student Records Policy
- Social Security Number and GWid Usage Policy

Additional University policies may be found at www.policy.gwu.edu.

Contact

If you have any questions regarding this policy or GW's websites generally, please contact us at comments@gwu.edu.

Appendix N

Privacy Policy

The George Washington University is committed to respecting users of GW's websites. For that purpose, this policy has been adopted to address the collection and use of information from GW's websites. In order to maintain effective privacy practices, GW retains the right to update this policy without notice.

Information Gathering

GW collects two types of information from users: (1) Information provided by the user in order to receive requested information and/or services, and (2) Information passively collected upon a user's visit to GW's websites.

Passively Collected Information

When a user visits one of GW's websites, some information such as the visitor's Internet protocol (IP) address, Internet service provider, operating system, the site from which the visitor arrived, and the time and date of the user's visit may be collected automatically as part of the software operation of the website. This intake of information is not personally identifiable. GW uses this information solely for internal purposes, such as, to see what pages are most frequently visited, in order to improve the site. Additionally, GW is currently using Google Analytics, a web metrics service, to collect certain information automatically upon a user's visit. For more information regarding Google Analytics, see Google's privacy policy.

Information Provided by the User

Users may provide GW with non-personally and personally identifiable information in order to utilize certain services and retrieve information. Such instances may not be noticeable to the user and include, but are not limited to: filling out surveys, purchasing goods and services, submitting tests, registering for courses, and submitting certain online forms.

Should the user choose to provide GW with any personal information, GW will use such information only to conduct official University business and will disclose it only when such disclosure may be appropriate to comply with applicable law, to enforce GW's Visitor Agreement, or to protect the rights, property or the safety of visitors to GW's websites, the University community or the public. GW does not sell, trade, or rent users' personal information to others.

Bibliography

American Library Association. (2007, October 26). Privacy Tool Kit. Retrieved from http: http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/default.

Angulo, J., Fischer-Hubner, S., Wastlund, E., & Pulls, T. (2012). Towards usable privacy policy display and management.*Information Management and Computer Security, 20*(1), 4-17. doi: http://dx.doi.org/10.1108/09685221211219155.

Babbie, E.*The Practice of Social Research*, 12th edition, Thomson 2012.

Burkell, J., & Carey, R. (2011). Personal Information and the Public Library: Compliance with Fair Information Practice Principles. Canadian Journal Of Information & Library Sciences, 35(1), 1-16.

Carnegie Foundation for the Advancement of Teaching (2010). The Carnegie Classification of Institutions of Higher Education. Retrieved from: http://classifications.carnegiefoundation.org/.

Carnegie Foundation for the Advancement of Teaching. (2013). Classifications Data File [Data file]. Retrieved from http://classifications.carnegiefoundation.org/resources/ .

Carter, H. (2002). Misuse of Library Public Access Computers: Balancing Privacy, Accountability, and Security. Journal Of Library Administration, 36(4), 29-48.

Crawford, W. (2005). THINKING IN POLICY TERMS. Library Technology Reports, 41(2), 4-10.

Dixon, P. (2008). Ethical Issues Implicit in Library Authentication and Access Management: Risks and Best Practices. Journal Of Library Administration, 47(3/4), 141-162.

Falk, H. (2004). Privacy in libraries, The Electronic Library, 22(3), 281 – 284.

Fifarek, A. (2002). Technology and privacy in the academic library. Online Information Review, 26(6), 366 – 374.

Fouty K. Online Patron Records and Privacy: Service vs. Security. Journal Of Academic Librarianship [serial online]. January 1, 1993;19(5):289-93. Available from: ERIC, Ipswich, MA. Accessed November 1, 2012.

Holmstrom, J. (2004). Managing a paradigm shift - Aligning management, privacy policy, technology and standards. Lecture notes in computer science, 3232, 442 – 451.

Innocenti, P., Vullo, G., & Ross, S. (2010). Towards a Digital Library Policy and Quality Interoperability Framework: The DL.org Project. New Review Of Information Networking, 15(1), 29-53. doi:10.1080/13614571003751071.

Jones, B. M. (2010). Libraries, Technology, and the Culture of Privacy: A Global Perspective. Library Technology Reports, 46(8), 8-12.

Kern, M., & Phetteplace, E. (2012). Hardening the Browser. Reference & User Services Quarterly, 51(3), 210-214.

Kooy, B. K., & Steiner, S. K. (2010). Protection, not barriers: Using social software policies to guide and safeguard students and employees. Reference & User Services Quarterly, 50(1), 59-71. Retrieved from http://search.proquest.com/docview/818634679?accountid=14244.

Million, A. C., & Fisher, K. N. (1986). Library records: a review of confidentiality laws and policies. Journal of Academic Librarianship, 11(6), 346–349.

Neuhaus, P. (2003). Privacy and confidentiality in digital reference. Reference and User Services Quarterly, 43(1), 26–36.

Sutlieff, L., & Chelin, J. (2010). 'An absolute prerequisite': The importance of user privacy and trust in maintaining academic freedom at the library. Journal of Librarianship and Information Science, 42(3), 163-177. doi: http://dx.doi.org/10.1177/0961000610368916.

Norden, D. F. (2003). FILTERING OUT PROTECTION: THE LAW, THE LIBRARY, AND OUR LEGACIES. Case Western Reserve Law Review, 53(3), 767.

Lofgren, K., & Webster, C. W. (2009). Policy innovation, convergence and divergence: Considering the policy transfer regulating privacy and data protection in three european countries. *Information Polity*, *14*(4), 295-314. Retrieved from http://search.proquest.com/docview/758112374?accountid=14244.

Magi, T. J. (2010). A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards?. College & Research Libraries, 71(3), 254-272.

Matz, C. (2008). Libraries and the USA Patriot Act: Values in Conflict. Journal Of Library Administration, 47(3/4), 69-87.

Neundorf, A. The Content Analysis Guidebook, Sage, 2002.

Nicholson, S. (2003). Avoiding the Great Data-Wipe of Ought-Three. American Libraries, 34(9), p. 36.

P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI 2010.

Reutty, M. (2007). What happened to me when the police came knocking. Computers In Libraries, 27(6), 10.

Shuler, J. (2004). INFORMATION POLICY Privacy and Academic Libraries: Widening the Frame of Discussion. Journal Of Academic Librarianship, 30(2), 157-159.

Stevens, N. (1994). Public libraries and the internet: Study results, policy issues, and recommendations. Government Information Quarterly, 1995, 12(2), 237-238.

62 pages. Retrieved from: (http://www.sciencedirect.com/science/article/pii/0740624X95900713).

US Supreme Court & Courts of Appeals Cases. JOHN DOE, Petitioner v. ALBERTO R. GONZALES, ATTORNEY GENERAL, et al. SUPREME COURT OF THE UNITED STATES. October 7, 2005. No. 05A295. 126 S. Ct. 1; 2005. Online. U.S. LEXIS 7258.

Vaughan, J. Toward a Record Retention Policy. (2007). The Journal of Academic Librarianship, 33(2). 217–227.

Voeller, S. (2007). Privacy Policy Assessment for the Livingston Lord Library at Minnesota State University Moorhead. Library Philosophy & Practice, 2007,1-29.