Web Privacy Policies in Higher Education: How Are Content and Design Used to Provide Notice (Or a Lack Thereof) to Users?

Anna L. Langhorne

University of Dayton, Department of Communication,
300 College Park, Dayton, Ohio 45469-1410
Alanghorne1@udayton.edu

Abstract. This paper explores the content themes and provision structures of the website privacy policies of a nonrandom sample of comparable universities across the United States. Because these organizations collect, analyze, and manage personal information via digital media, it is important to evaluate the legal content and usability of their privacy policies. The issue is complex, because technology continues to advance, privacy policy standards continue to evolve, and the law is unclear on many aspects of privacy. Furthermore, the education sector lags industry in its implementation of privacy and security programs. A content analysis was conducted to identify patterns in legal provisions, general usability, and communication of sixteen university web privacy policies. This approach revealed what universities disclose about their information practices and user rights. The results reveal the commonalities of how web privacy policies are structured, what concepts are presented, and what information is absent. Additionally, recommendations are shared regarding how to develop comprehensive online privacy policies appropriate for higher education.

Keywords: Privacy, privacy policy, privacy law, information practices, security, usability, higher education, information sharing, communication, cyber security.

1 Introduction

Higher education websites serve as global communication vehicles, connecting content and materials with domestic and international audiences (e.g., prospective students/parents, enrolled students and their parents, employees, alumni, and community members). Interactions between users and university websites create many opportunities for data generation and collection. For example, many websites passively collect data about users, such as page visits and referring websites. These data may be anonymous or identified. In addition, data may be actively collected. An example is when a user voluntarily shares data through site registration to complete an information request. The nature of these data may be nonspecific but may involve personal information (PI). PII data is involved when a user shares personally

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 422–432, 2014.

identifiable information (e.g., prospective student discloses her Social Security Number in an online application), something that occurs when a tax return is submitted for financial aid consideration, or perhaps health the submission of immunization records

These examples represent a limited sample of the many ways in which university websites touch user data. The situation becomes more complex when one considers how and with whom information is shared. Higher education institutions share information with third parties with increasing frequency. These associations include, but are not limited to, parties such as advertising providers, vendor partnerships, or law enforcement. For example, the University of Iowa had a data sharing relationship with the local sheriff's office. After the sheriff notified the university that a student applied for a gun permit, the university allowed the sharing of information related to academic performance and emotional state [1]. Through these kinds of arrangements and data generating activities, universities have become custodians of massive amounts of PI and non-PI. As stewards, they assume a duty to protect that information.

Privacy policies (PPs) are official communications through which organizations disclose their information practices and approaches to privacy and data protection. Given current societal concerns, higher education websites should provide and be governed by online PPs. These policies can be designed to meet university legal compliance needs as well as provide meaningful notice to users. When they are effective and successful, they also have the potential to build user trust. In essence, PPs are communication opportunities to inform, assure, and empower users. Therefore, PPs may aid relationship development between institutions and users. Trust and relationship building are important as higher education continues to learn lessons about the impact of inadequate (or nonexistent) privacy and security programs. The 2006 hack of Ohio University's databases and theft of 173,000 Social Security numbers illustrate how brand erosion, relationship damage, and diminished profitability may result. Ohio University sustained a class action lawsuit and an 8% decline in donations compared to the previous year [2]. More recently on February 19, 2014, the University of Maryland announced it was hacked [3]. The records of 309,079 student, faculty, and staff were compromised, many of whom were affiliated as long ago as 1998. Their names, Social Security Numbers, birthdates, and university IDs were divulged.

These concerns about privacy and security and the impact on university brand and user trust are now part of the higher education privacy landscape, in which several factors are relevant. First, there is a trend to move information and documents to an electronic format, and as the University of Maryland example illustrates, these records are attractive to potential criminals and wrongdoers. As a result, there are risks and vulnerabilities associated with collecting, using, managing, and storing records in digital environments, regardless of whether the records comprise PI or non-PI. Privacy and security concerns are well founded due to an increase in breaches across sectors; however, higher education contributed "nearly 160 breaches and more than 2.3 million records breached since 2008" [4].

Unfortunately, the current legal structure is unprepared to cope with privacy and security needs. Currently, forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification legislation [5]. Many laws stipulate aspects of breach disclosures such as procedures and timing, although they vary in terms of specificity. In 2011, FERPA allowed authorized representatives to share student personal information without consent, making it easier to share information with nongovernmental actors [6]. However, regulatory changes are moving toward expanded requirements for the private and public sectors (e.g., HIPAA requires institutions to have a privacy officer). California recently passed a privacy law which prohibits public and private postsecondary educational institutions from requiring or requesting student disclosure of social media information including: 1) username or password, 2) access in the presence of the institution's member, or 3) personal social media information [7]. Changes are inevitable as the FTC clarifies standards for industry.

Third, there is an expanding focus on big data and analytics and new technologies that challenge traditional notions of privacy. Social media, for example, blur the lines of organizational boundaries and create complexities in information management and protocol. Not only are there diverse types of data and invasive technologies, but higher education, and universities in particular, have complex interactions with data. Given the numerous potential university units that touch website data (e.g., marketing, admissions, financial aid, student affairs, human resources, institutional research, information security, campus police, and library services), privacy issues are both highly sensitive and extremely important.

The purpose of this descriptive study is to determine the nature and extent of information practice disclosure via university website privacy policies. A content analysis was conducted of sixteen university PPs. The objectives are: 1) Describe commonalities in web privacy policy content and design, 2) Identify differences in approaches to privacy, 3) Contrast the policies with FTC recommendations for fair information practices, and 4) Provide recommendations for improving higher education online privacy.

2 Literature Review

2.1 Usable Online Privacy Policies and Their Value

Usability refers to the ease of use, learnability, efficiency, memorability and satisfaction of a system. It is the measure of quality of a user's experience. In the context of online privacy policies, usability means a policy should be easy to locate, easy to read, and quickly digestible. It should provide useful information that is needed by users. Finally, it should empower users to make informed decisions about their online behavior.

Unfortunately, most PPs are overwhelmingly unsatisfactory. Many policies are dense and written in legalese, exceeding the reading level of users [8]. The resulting incomprehensibility of PPs prevents the organization from successfully giving notice to the user. The challenges associated with online privacy policy design include the understandability of jargon and privacy preference complexity [9], user fatigue issues due to reading difficulty and time consumption [10], improving organization trustworthiness [11], policy effectiveness related to brevity, clarity, and breadth [12], and format effect on comprehension [13].

PP effectiveness is based on several factors. The Article 29 Data Protection Working Party recommends a multilayered format in which an initial webpage provides summary notice with primary information, where detailed information is provided via subsequent webpages [14]. Alternatively, Kelley et al. (2009) suggest modeling privacy policies after nutrition labels to improve the accuracy and efficiency of locating relevant information [15]. Angulo et al (2012) articulated an approach for designing user-friendly privacy policy interfaces which incorporated a nutrition label format with the added features of privacy alerts (e.g., notification of identified third-party data sharing and usage) and parallel privacy management (i.e., users could adjust privacy settings “on the fly”) [16]. They found users valued the ability to manage their privacy during web interactions. However, results also revealed the difficulty in balancing design, content, and attention demands. Similarly, a study of online behavioral advertising notices (OBAs) found notices go unnoticed by users, ineffectively communicate user choices, and fail to inform users about the choice mechanisms OBAs provide [17].

When effectively designed, PPs provide organizational value. In addition to satisfying legal compliance, it may influence user attitudes about the organization and choices about disclosure. In an examination of privacy, Xu et al (2011) determined organizational factors, such as privacy policies, and user attitudes and perceptions are related to privacy concerns [18]. In a related study of consumer trust, Flavian & Guinaliu (2006) found “trust in the Internet is particularly influenced by the security perceived by consumers regarding the handling of their private data by the website (p. 612) [19]. Privacy policies may function to alleviate user privacy concerns.

3 Methodology

3.1 Sample

A nonrandom sample of twenty-eight higher education institutions was selected (See Table 1). All university websites’ homepages were reviewed for a link to a privacy policy. If no link was provided, the website was searched internally to identify whether a privacy policy existed. Fordham University, Loyola University Chicago, and Saint Louis University were excluded after a search of their websites yielded no results. Although the remaining twenty-five websites provided privacy policies, many addressed areas unrelated to the focus of this research paper (e.g., alumni relations, library services, health center, registrar, and online programs). Only sixteen university websites provided a web or combination privacy policy (i.e., a privacy policy that addressed numerous areas, including the website) (See Table 3).

Table 1. Sample of university websites

University	URL	Privacy Policy Type
American University	www.american.edu	Combination
Baylor University	www.baylor.edu	Combination
Bradley University	www.bradley.edu	Other
Creighton University	www.creighton.edu	Other
Depaul University	www.depaul.edu	Other
Drexel University	www.drexel.edu	Web
Duquesne University	www.duq.edu	Web
Fordham University	www.fordham.edu	N/A
Hofstra University	www.hofstra.edu	Other
Lehigh University	www4.lehigh.edu	Web
Loyola Marymount University	www.lmu.edu	Web
Loyola University Chicago	www.luc.edu	N/A
Marquette University	www.marquette.edu	Web
Miami University	miamioh.edu	Combination
Ohio University	www.ohio.edu	Other
St. John's University	www.stjohns.edu	Other
St. Joseph University	www.sju.edu	Other
Saint Louis University	www.slu.edu	N/A
Santa Clara University	www.scu.edu	Web
Seton Hall University	www.shu.edu	Web
The Catholic University of America	www.cua.edu	Other
The Ohio State University	www.osu.edu	Web
University of Cincinnati	www.uc.edu	Other
University of Dayton	www.udayton.edu	Web
University of Denver	www.du.edu	Combination
University of San Diego	www.sandiego.edu	Web
Villanova University	www.villanova.edu	Web
Xavier University	www.xavier.edu	Web

3.2 Data

Two types of data were gathered from the selected university website privacy policy pages. First, the policies received a usability score based on whether a policy feature or design characteristic was present according to a 16-point checklist (See Table 2). Second, the text of the privacy policy text was captured and the content was analyzed. The data collection was performed from November 2013 to February 2014.

3.3 Content Analysis

Content analysis was used to examine the website and combination PPs of sixteen universities. The content was analyzed using a coding scheme that incorporated measures of usability, communication, fair information practice compliance, and legal concepts. The unit of analysis was the concept or feature. If a concept (e.g., a legal provision) or feature (e.g., a homepage link to PP) was present, it was coded as a one. Absent concepts/features were coded as zeros.

Table 2. Privacy Policy Coding Scheme – Abridged Version

SAMPLE MEASURES	
General categories	**Examples of concepts/features**
Usability	Homepage link, privacy policy label, layered format, contrast, font size, heading/sub-headings, bullets, clear policy purpose, critical information above fold, icons
Communication	Policy steward, contact information, links – related policies, links – related resources, definitions, notifications, plain language
Fair Information Practices	Notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress
Legal	Provision types, obligations, user rights, consent mechanisms, procedures, policy violation, regulations/frameworks, standards

The coding scheme addressed PP usability, communication openness, fair information practices, and legal orientation. The usability measures ranged from navigation (e.g., whether there was a direct path to the PP) to page and content design (e.g., PP layout, scannability, and chunking). Communication focused on openness (e.g., identifying a named privacy officer), clarity of concepts (e.g., definition usage), and facilitation of interactions (e.g., contact phone number or email address). The fair information practices category comprised concepts related to data collection, usage, storage, protection, sharing, and management (e.g., user access to stored data). The legal category facilitated classification of PP provision types, whether procedures were stated, and what regulatory frameworks were identified.

3.4 Coding Process and Data Analysis

Policies were coded for the presence or absence of features, concepts, themes, and provisions. A present entity was coded as 1. Absent entities received a 0. Policies occasionally referenced third-party privacy policies. In those examples, it was noted there was third-party policy content, but it was not coded as part of the university policy. Similarly, online PPs solely focused on specific departments (e.g., spirit, library use, alumni networks, health center, or student records) were excluded from coding, although it was noted the policy existed for the department/function. The focus of this analysis was web PPs and comprehensive PPs.

After coding the PPs, a percentage was calculated of PP entities present within each of the categories. The total number of possible features/concepts follows: Usability (16), communication (30), fair information practices (164), and legal (49).

The percentage represents the PP emphasis of certain concepts, features, and focuses. For example, a usability score of 100% indicates the PP addressed or met 16 of the 16 possible measures. Although a high percentage is expected to correlate with satisfactory usability, it does not represent a passing or failing score.

4 Results and Discussion

Overall, the results illustrate too many universities have no website/combination PP (43% of the universities sampled for this study), which prevent universities from reassuring their customers and building their brands and images [20]. Equally troubling is the serious need for improvement across all focus areas: Usability, communication, fair information practices, and legal content. No PP excelled in every area. In fact, usability is the only category where some PPs showed strength. All PPs were weak in the areas of communication, fair information practices, and legal concepts.

Table 3. Privacy Policy Content Analysis Results

University	**Usability (16 items)**	**Communication (30 items)**	**Fair Information Practices (164 items)**	**Legal (49 items)**
American University	50%	3%	13%	4%
Baylor University	50%	7%	18%	6%
Drexel University	69%	3%	10%	4%
Duquesne University	38%	7%	12%	4%
Lehigh University	31%	7%	15%	4%
Loyola Marymount University	69%	0%	15%	2%
Marquette University	56%	3%	15%	4%
Miami University	63%	7%	18%	6%
Santa Clara University	0%	7%	12%	0%
Seton Hall University	0%	3%	8%	0%
The Ohio State University	31%	0%	4%	0%
University of Dayton	44%	7%	14%	8%
University of Denver	38%	10%	12%	2%
University of San Diego	63%	10%	12%	4%
Villanova University	56%	0%	13%	2%
Xavier University	6%	7%	17%	10%
Mean percentage across PPs for each category:	**43%**	**5%**	**13%**	**4%**

Regarding usability, the mean score was 43% with a range from 0% to 69% (See Table 3). Most PPs used high text/background contrast and headings (87.5% and 69%, respectively), and adopted plain language (81%). However, a minority of policies provided a clear path to contact information (37.5%), used a layered format (0%), used subheadings (6%) and icons (0%), placed critical content above the fold (12.5%), or provided concise provisions (25%). Thirty-eight percent of universities had no homepage link to the PP, forcing users to search for, and perhaps not find, the PP. The good news is the aforementioned inadequacies have simple solutions: Add a homepage link, place a summary of important information above the fold, reduce the amount of text in provisions, and use bullet points to make information digestible.

Communication focused on whether a PP provided openness, concept clarity, and means for interaction. All PPs lacked a communication focus, shown by the overall mean score of 5% and a high score of 10%. Few PPs provided links to related policies (31%) and resources (0%). None of the policies identified a privacy officer or privacy office. Perhaps this indicates an absence of a dedicated, formalized approach to privacy. Although 62.5% provided contact information, it was usually a generic email (e.g., webmaster@university.edu) or a mailing address. Only 12.5% of the PPs provided definitions of key terms like personal information, education record, and third-party. Finally, every PP failed to address communication related to breaches, violations, and corrective action. In general, universities failed to use the PP as a communication opportunity. To improve, PPs should identify the privacy officer and provide multiple methods for communication. They should define jargon and share information about university communication and notifications.

The fair information practices category showed university PPs do not adequately reflect the FTC concepts of notice, choice, access, integrity, and enforcement. The university PPs, with a mean score of 13%, neglected to address many important topics. Although 87.5% of PPs mentioned data collection such as general cookies (62.5%), log files (37.5%), and web servers (25%), no policies differentiated among cookie types, explained the collection process, or provided detailed information about the collection process. Similarly, PPs frequently referred to PI (75%), web page visitation (62.5%), and IP address (81%), but few if any PPs were specific about the PI or provided information on other data types such as health, education, and social media. PPs also failed to provide notice about data usage (e.g., marketing - 19%, behavioral advertising – 0%, and association with other data – 19%) or data storage. PPs generally omitted information about what information is stored, how long data are retained, and archival/destruction methods. In terms of data protection, PPs mentioned general safeguarding (44%) and encryption (50%), but neglected the concepts of compliance reviews (0%), audits (6%), physical security (6%), privacy programs (0%), verifications (0%), vulnerability testing (0%), and anonymizing data (0%). The policies also sparsely referenced or discussed data management. No PP discussed general opting out. Few data management options were presented and were limited to opting out of third-party sharing (6%) and communication (25%). Data sharing was another troubling area. Only 56% of PPs stated there was no selling of data and no policies were clear about how data was shared across the university. All PPs failed to discuss how a user could access his data or recourse methods. University

PPs could better reflect fair information principles by providing more transparency and detail about data collection, management, sharing, and storage practices.

The legal category allowed classification of PP provision types, procedures, PP history, and regulatory frameworks. University PPs, with a mean score of 4%, did not address legal concepts as defined here. Although 81% addressed miscellaneous provisions, the focus was on disclaiming responsibility for the university website (62.5%) or external websites (62.5%). No PPs stated procedures for general inquiries, reporting incidents, filing complaints, or requesting status updates. No policies addressed prohibited activities such as identity theft, and policy violation remedies were absent (termination, expulsion, training, ID theft prevention protection). Regarding PP history, only 31% shared an effective date and a revision date. Finally, PPs infrequently referred to regulatory frameworks, with mentions solely of HIPAA (12.5%), general state law (12.5%), or the Ohio Public Records Act (6%).

5 Future Research and Limitations

This research establishes a comprehensive framework for evaluating PPs in terms of usability, communication, fair information practices, and legal perspectives. Although the content analysis provided a broader and deeper investigation of PP content than other content analyses [2, 21, 22, 23], the coding scheme can benefit from additional refinement. In future research, the coding scheme will be revised to provide an assessment of how well the PP addressed concepts. In addition, experimental research should be conducted to determine PP effectiveness.

In terms of limitations, capturing PPs presents challenges. As this study showed, many organizations fail to include a direct link to the PP from the homepage. This forced the use of internal and external search engines to locate PPs. It is possible that an organization may have a PP even though it was not located. Of course, this raises an important issue: Users need to be able to locate PPs in order to have notice of the information practices. Another limitation relates to the disorganization of PP content. Because there are limited PP best practices and no standards, content is highly variable and policies differ in provisions placement and sequence. In fact, many policies use vague, informal language and have no defined provisions. This presents an issue content coding. In the present study, if a concept was present, it received credit. This issue can be addressed by including subjective measures in future coding frameworks.

6 Conclusion and Recommendations

University website/combination PPs provide inadequate notice to users. They fail to address the complex issues and situations that originate from universities assuming the role of information steward. The duties that accompany the steward role are not reflected in the language or structure of privacy policies. This was demonstrated by the tendency of university PP content to ignore communication standards, fair information practices, and important legal information.

Good privacy policy design is an expectation and a requirement, especially given the level of sensitivity of some information activities in higher education. Institutions should develop PPs that address the needs of their constituents. They need to be written in plain language, organized, comprehensive, and informative. A few areas to improve: 1.) Provide transparency about the collection, usage, sharing, and storage of information, 2.) Provide access to the information and articulate the mechanism for addressing privacy issues (e.g., correcting data, reporting violations), and 3.) Give users choice regarding the disposition of their data. Higher education institutions also should provide information on privacy topics of specific concern to education (e.g., affiliation of education record data with browsing behavior).

Usable PPs are feasible for all education institutions as they can be economically developed and produced [24]. It is a low investment that may alleviate user privacy concerns and improve user perceptions of risk and control. This preventive measure is an investment in reputation management and proactive alleviation of harm/damage. There are several easy, low-cost ways to create or improve policies.

A concise, comprehensive privacy policy that meaningfully addresses user needs is an opportunity for an institution to demonstrate its commitment to user privacy, an understanding of its data governance, accountability, and an interest in trust building. Given the relatively low cost of developing and communicating such a policy, universities would be well advised to invest a small amount of resources in exchange for a significant return in the future.

References

1. DeSantis, N.: U. of Iowa Shares Data With Local Sheriff on Students Seeking Gun Permits. The Chronicle of Higher Education (December 17, 2013)
2. Culnan, M., Carlin, T.: Online Privacy Practices in Higher Education: Making the Grade? Communications of the ACM 52(2), 126–130 (2009)
3. Loh, W.: UMD Data Breach (2014), http://uhr.umd.edu/2014/02/umd-data-breach
4. Cox, J.: Are Colleges and Universities at Greater Risk of Data Breaches? Network World (2010), http://www.networkworld.com/news/2010/091510-higher-ed-data-breaches.html
5. National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (retrieved February 2, 2014)
6. FERPA, 34 C.F.R. section 99.3 (2011)
7. California Social Media Privacy Law S.B. 1394 (2012)
8. Jensen, C., Potts, C.: Privacy Policies as Decision-making Tools: An Evaluation of Online Privacy Notices. Paper presented at the CHI 2004, Vienna, Austria (2004)
9. Cranor, L., Guduru, P., Arjula, M.: User Interfaces for Privacy Agents. ACM Transactions on Computer-Human Interaction 13(2), 135–178 (2006)
10. McDonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F.: A Comparative Study of Online Privacy Policies and Formats. In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 37–55. Springer, Heidelberg (2009)

11. Au, N., Law, R.: Presentation Formats of Policy Statements On Hotel Websites and Privacy Concerns: A Multimedia Learning Theory Perspective. Journal of Hospitality & Tourism Research (2012)
12. Goel, S., Chengalur-Smith, I.N.: Metrics for Characterizing the Form of Security Policies. The Journal of Strategic Information Systems 19(4), 281–295 (2010)
13. Vail, M.W., Earp, J.B., Antón, A.I.: An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. IEEE Transactions on Engineering Management 55(3), 442–454 (2008)
14. Article 29 Data protection Working Party, Opinion on More Harmonised Information Provisions 1198704/EN WP 100, European Commission (2004)
15. Kelley, P., Cesca, L., Bresee, J., Cranor, L.: Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, p. 1573. ACM, New York (2010)
16. Angulo, J., Fishcer-Hübner, S., Wästlund, E., Pulls, T.: Toward Usable Privacy Policy Display and Management. Information Management & Computer Security 20(1), 4–17 (2012)
17. Leon, P., Cranshaw, J., Cranor, L., Graves, J., Hastak, M., Ur, B., Guzi, X.: What Do Online Behavioral Advertising Disclosures Communicat to Users? Carnegie Mellon University CyLab (2012)
18. Heng, X., Dinev, T., Smith, J., Hart, P.: Information privacy Concerns: Linking Indivdiual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12(12), 798–824 (2011)
19. Flavián, C., Guinalíu, M.: Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site. Industrial Management & Data Systems 106(5), 601–620 (2006)
20. McRobb, S., Rogerson, S.: Are They Really Listening? An Investigation Into Published Online Privacy Policies at The Beginning of The Third Millennium. Information Technology & People 17(4), 442–461 (2004)
21. Reay, I., Beatty, P., Dick, S., Miller, J.: Privacy Policies and National Culture on the Internet. Inf. Syst. Front. 15, 279–292 (2013)
22. Jensen, C., Potts, C.: Private Policies Examined: Fair Warning or Fair Game? (2003)
23. Earp, J.B., Antón, A.I., Aiman-Smith, L., Stufflebeam, W.H.: Examining Internet Privacy Policies within the Context of User Privacy Values. IEEE Transactions on Engineering Management 52(2), 227–237 (2005)
24. Meinert, D., Peterson, D., Criswell, J., Crossland, M.: Privacy Policy Statements and Consumer Willingness to Provide Persona Information. Journal of Electronic Commerce in Organizations 4, 1–17 (2006)