

Data Protection in the University Setting: Employee Perceptions of Student Privacy

Julia B. Earp *North Carolina State University* Julia_earp@ncsu.edu
Fay C. Payton *North Carolina State University* Fay_Payton@ncsu.edu

Abstract

The right to privacy is not absolute and is often established by context and the need to know. The nature of the university environment sometimes distorts the sanctity of privacy because the "need to know" is so profuse. Although students are guaranteed the right to keep essential but confidential information private under the Family Educational Rights and Privacy Act of 1974, student data are vulnerable because of the need for academic departments to share and manage these data. Recent articles in the popular press suggest consumers as a whole are questioning organizational practices that are designed to protect their personal information. Similar practices occur in the university setting, but fewer concerns are being publicized. Because of the vast amount of data sharing that occurs in an academic setting, it is imperative that we ensure the employees adhere to privacy policies that are structured to impose conscientious behaviors. University privacy policies are in practice, but there is no method of determining their effectiveness. This research seeks to ascertain the attitudes of employees regarding student privacy. Using a 15-item instrument, this study explores employees' privacy perceptions of a large university located in the Southeastern U.S. Our study examines the level of concerns employees have concerning errors, unauthorized secondary use, improper access and collection.

1. Introduction

Implementations of information technology (IT) in the university setting have been well received in most cases. Information access has become more efficient in administrative areas such as admissions, the registrar's office, financial aid, advising, as well as campus security systems. Despite its effectiveness, the transmission and dissemination of student information in electronic form introduces a myriad of privacy concerns among students and academic administration, alike.

The evolving trend toward electronic student records has a proven potential for increased information sharing among departments within the university setting.

Furthermore, as electronic student records continue to become more ubiquitous, accessibility and sharing will become so easy that the effectiveness of university privacy policies will need to be ensured. Regarding invasions of student privacy and student records, university employees that create, store, use, and transmit student records are likely to know more than most. Given the heightened concern in privacy as a whole, universities will need to be sure that a positive relationship exists between their privacy policies and employees' attitudes and practices.

The issue of student privacy, as it pertains to organizational practices, holds profound implications as ubiquitous computing and innovative technologies become more abundant. While many continue to debate about what should be done to protect individual privacy, advocates such as EDUCAUSE, an association focused on university changes introduced by information technologies, seek to educate users and develop guidelines to discourage harmful acts involving personal information. Organizational privacy policies articulate these guidelines, but the objectives often appear conflicting - as employees are unclear (or unaware) of their roles in guarding student information and privacy.

Some researchers [7] have realized the need for validated instruments for measuring individuals' concerns about organizational practices and therefore, developed tools to identify and measure the principal dimensions of privacy concerns. Given the concerns of the general population and the innovative technologies being introduced to university environments, we have applied these validated tools to explore how university employees assess the practices of their organizations. Understanding the attitudes of employees who have regular access to personal information will assist the field in developing better methods for privacy protection as universities continue advancing into ubiquitous computing environments.

2. Current Practices and Literature Review

The literature shows that organizations, including universities, have a significant degree of concern

regarding privacy and how IT can enable/hinder individuals' abilities to safeguard information [3]. Given the evolving trends in university settings, the degree to which universities adhere to privacy policies plays a key role in the effectiveness of record keeping among the implementations of student records, security measures and legal policies. Earlier works have added to the knowledge of privacy concepts and legal interpretations, but until now the perceptions of university employees regarding organizational practices has been neglected. Such perceptions will provide the field with a basis for analyzing privacy practices as universities continue implementing innovative computing technologies.

Due to its compact nature, the campus environment is ideal for exploiting innovative ubiquitous computing technologies. As these technologies improve, students will begin using them in a variety of situations. Wireless technologies will tell students where they are on campus and provide directions, classroom location, course specific information, and personal information regarding food services [9]. Some universities are already employing the use of handheld computers to assist in course delivery. For example, the eClass Project at Georgia Tech is studying ubiquitous computing in the university environment. They are using palmtop computers to capture student notes during lectures, then synchronizing that information with audio/video from the instructor's lecture and stored on the Web. (see <http://www.cc.gatech.edu/fce/eclass/>).

Another innovative technology achieving acceptance in many U.S. university settings is the smart card. With smart card implementations rising, potential privacy concerns are becoming a most important issue. Smart cards are currently being used at FSU, Washington University and University of Michigan. The University of Michigan employs a single-card program that combines features such as identification, library privileges, building access, meal plans, long distance calling, and debit features. Similar cards have been issued to students, faculty, staff, and visitors at other schools as well.

Princeton University upgraded its access controls to 24 hour security systems for the New Jersey campus in 1997. In addition to the technological challenges faced by the developers, the privacy concerns of the students proved even more difficult. The students were concerned that their privacy would be compromised by the new system. They were opposed to the initial system and asked the university to ensure that it would not use the database of access card entries for tracking student movements. As a result of the student demands, the university altered the system to act as an ingress reader only and developed a formal privacy policy that governs the use of the access

control data. The data is currently available for maintenance and on a "need to know" basis [8]. Logging and monitoring are introducing new privacy concerns to university environments. Students will eventually give up a degree of privacy in the interest of security.

The regulations regarding privacy in academia are set by law and institutional policy, but members of NACADA (National Academic Advising Association) believe that many relevant employees are unaware of them. For this reason, the association promotes policy education university wide. The mission of NACADA seeks to anticipate the academic advising needs of the twenty-first century [6]; therefore, its members recognize the increasing dilemmas being introduced through computerized student records. For this reason, they continue to advocate the importance of strong university ethical foundations and dedicate a portion of their national conferences to ethical and legal issues.

Although the Family Educational Right to Privacy Act of 1974 (FERPA) aims to protect the privacy of student records, various occurrences have arisen to test the extent of this law. The Act provides students the right to inspect education records, the right to request to amend those records, and to limit disclosure. However, a report by CAUSE [2] maintains that FERPA will not continue to effectively protect students of privacy violations in the modern electronic environment. The CAUSE report [2] outlines the privacy challenges being encountered by universities involved in technological advances. The conclusion of the report is a recommendation that "...each college and university engage in a process to clarify the values that generally reflect its unique culture, mission, and environment." This research seeks to address this recommendation by identifying the privacy values held by relevant university employees.

In 1998, Ohio State University and Miami University were thought to be in violation of the Family Educational Rights and Privacy Act (FERPA). They were releasing campus crime records that included student names [5]. As a result of the Ohio incidents, in 1999 the U.S. Education Department proposed rules to loosen student-privacy laws. The proposal was founded on programs to crack down on student drug and alcohol abuse and crimes. It suggested creating guidelines under which colleges could disclose information about crimes, alcohol abuse and drug abuse [1].

In addition to general education records, universities also maintain sole-possession records not protected under FERPA. Examples include records of employment by the institution, physician records, psychiatrist records, campus security records, and other records created from

new technologies. Using computer information systems to maintain student records is becoming a normal approach for university record keeping in all areas. Although universities establish policies to protect the confidentiality of various types of student records and educate faculty and staff, we currently have no basis to understand the protective actions of these employees. The significance of this understanding will grow as universities involve themselves in more computerized environments. Eventually the threat to privacy protections beyond campus boundaries will become a risk [10].

Because employees of any organization are ultimately in control of sensitive customer (or student) information, it is important to understand employee attitudes, as well as consumer (student) attitudes, toward privacy. Thus, the information systems field is in need of research that explores individuals' perceptions of organizational information privacy practices [7]. [7] previously explored privacy concerns of *consumers* in a heterogeneous setting. Our study is unique as it utilizes a university setting to "measure" privacy perceptions of *employees* having daily exposure to information processing activities. Earp and Payton [4] analyzed a parallel concept in the health care setting and discovered health care employees to be highly concerned with errors in patient records - as errors can lead to life threatening consequences and even death. **We hypothesize that university employees are largely concerned about the collection of and errors in student information - as academic settings are largely data warehouses of student information typically dispersed throughout numerous, autonomous departments. Thus, we seek to explore the perceptions of university employees regarding the privacy of student information.** The results of this study will then be compared to those of Smith, et al. [7].

3. Methodology

We administered a 15-item instrument (See Appendix) and cover letter to 160 university employees who have daily exposure as well as access to student information. While these employees did not include university faculty, our subjects are staff from diverse departments including: 1) student health services, 2) registration and records, 3) public safety, 4) student advising, 5) legal affairs, 6) administrative computing services, and 7) the counseling center. It should be noted, however, that the manager of the Information Technology (IT) Services would not comply to the survey and thus, our results do not include IT professionals that control student access to network services, such as email, college intranets and the World Wide Web (WWW). Due to limited communication with the IT Services manager, it is difficult to speculate as to why this happened, although it was indicated that the staff

had more critical issues to resolve. All participants are employed by a large Southeastern, public, land-grant university.

Prior to administering the survey instrument, we contacted departmental managers and requested their participation in this research. After which, graduate students coded each departments' surveys and hand-delivered all instruments in a large envelope to unit managers. Thus, this enabled us to gain a significant degree of top management support for and completion of our survey instruments.

Within a 7-day period, 144 usable surveys were returned resulting in a 90% response rate with nearly 15% returned from the Administrative Computing Services group. These data show that 27% (or 39) of our respondents were males while African and Hispanic Americans represented 41% of the subjects. None of the participants were less than 20 years, and less than 2% were over 60. Twenty-seven percent (27%) of the sample were between 41-50 years of age. Nearly 30% of the sample indicated that they had 7-10 years of experience in higher education.

4. Results

Table A shows how our items grouped by factor loadings, and the results indicate that four variables (Unauthorized Secondary Use, Errors, Collection and Improper Access) emerged from the survey instrument as shown in the Appendix. Additional information on these variables and their conceptual meanings are explained in Earp and Payton [4].

The described results are from the sample of 144 university staff. All loadings above 0.50 are listed in Table A, and our results indicate the presence of four factors: *Improper Access*, *Unauthorized Secondary Use*, *Errors* and *Collection*. Scale reliabilities for these factors are 0.91, 0.87, 0.67 and 0.46, respectively. An examination of total item correlations and a Varimax Factor Pattern led to the omission of Item J (*Bothers "subject" to give student info to others*; See Appendix) due to cross-loadings and poor scale reliabilities.

Most of the variance explained and reported in the eigenvalues for our data is done so by *Improper Access* reported at 3.94 and *Unauthorized Secondary Use* at 3.13. The variance explained by *Errors and Collection* are 1.81 and 1.65, respectively. In sum, the cumulative variance explained in Table A is 10.53 with over 33% attributed to the *Improper Access* dimension of privacy.

Table A: Factor loadings of data analysis

Item # & Description	IA	US	E	C
Steps to prevent unauthorized use in computers - N	0.85			
Procedures to correct errors in student info - H	0.84			
Time/effort to verify student info in databases - L	0.82			
Preventing unauthorized access - D	0.79			
Unauthorized persons cannot access student info - O	0.76			
Never use student info other than for care - G		0.82		
Never sell student info unless authorized - M		0.77		
Computer databases with student info are protected - I		0.75		
No use of student info for any purpose - C		0.62		
Think twice before recording student info - E		0.58		
Bothers "subject" to ask for student info - A			0.85	
Double check student info in databases - B			0.72	
Never sell student info in databases - K				0.77
Steps to ensure accuracy of student info - F				0.69

IA: Improper Access C: Collection
 US: Unauthorized Secondary Use E: Errors

The means and standard deviations of the responses are shown in Table B. On a 7-point scale, the responses are somewhat tight about the mean for all responses - with item A ("it bothers me when the university asks for student information") illustrating the lowest mean (4.159) and largest standard deviation (1.80). Conversely, item O ("collecting too much information about students") holds the highest mean value (6.40) and smallest standard deviation (1.16).

Table B: Mean and Standard Deviation of Responses

Var	Mean	Std Dev
A	4.15972	1.80389
B	5.20833	1.62530
C	5.15972	1.65002
D	5.83333	1.69739
E	5.64583	1.46028
F	4.29861	1.82477
G	5.59722	1.32917
H	6.05556	1.62918
I	5.30556	1.32368
J	6.06250	1.44464
K	5.33333	1.52829
L	6.29861	1.44880
M	5.50000	1.32749
N	6.23611	1.
O	6.40972	1.16122

Lastly, Table C shows the final instrument of the Smith, et al. [7] factor analysis. Note that this table is shown as published in *MIS Quarterly* [7].

A close examination of Tables A and C indicate that our results support the 4-factor concept of privacy as found by Smith, et al. [7]. Given the organizational setting for this research, our results suggest that academic professionals (who have daily exposure to student information) are largely concerned about the improper access of these data - thereby failing to support our initial hypothesis that they are most concerned about collection and errors. Further, our findings are bipolar in comparison to Smith, et al. [7] - as most of the variance explained in our exploratory model is done so by *Improper Access, Unauthorized Secondary Use, Errors and Collection*, respectively. The Smith, et al. [7] study found that *Collection, Errors, Unauthorized Secondary Use and Improper Access*, respectively, supported their work.

Table C: Factor loadings from Smith, et al., 1996

Item	C	E	US	IA
J	.861			
E	.856			
A	.855			
O	.762			
F		.864		
H		.816		
L		.811		
B		.679		
K			.778	
M			.768	
G			.719	
C			.717	
N				.773
D				.771
I				.719

IA: Improper Access C: Collection
 US: Unauthorized Secondary Use E: Errors

Moreover, the omission of Item J ("*Bothers me to give student information to other organizations*") can be interpreted in several ways:

- 1) The item was poorly worded for an academic setting where organization can be mistaken for Fortune 500, corporate, etc. settings
- 2) Organizations can, likewise, be interpreted as both departments and colleges between the university setting - thus, resulting in a myriad of meanings among the study's participants

Despite the withdrawal of Item J, our data supports the idea that privacy is a 4-factor construct, but as a general concept, privacy is not easily interpreted. Results of our work [4] from a health care organization resulted in a different factor structure suggesting the need for our work to extend into a confirmatory model and analysis framework.

5. Conclusions and Future Work

This study used a pre-established instrument to investigate the privacy perceptions of university employees who consistently handle confidential student information. While our study did address the research hypothesis, our findings suggest that academic employees are largely concerned about organizational practices that lead to and/or result in improper access and unsanctioned use of student information. Although issues of privacy abound, perceptions of organizational policies and practices appear to be significantly associated with university regulations and government mandates.

University information technology administrators can address issues of *improper access* and *unauthorized secondary use* of student information by ensuring that appropriate security and database technologies are implemented to protect privacy. Conflicts arise between organizational policies that call for a prescribed level of performance and the experience of workers (who have daily exposure to personal information) in the collection, access and use of such data. Thus, worker roles and responsibilities should be clearly articulated and reconciled with organizational policies.

Another phase of this study will explore the student perspective about university privacy. A corresponding questionnaire will be used to ask students about their concerns and opinions. Privacy, as it relates to students, is a central focus to the study - therefore, comparing such information to that reported in this manuscript could provide some interesting inferences to the results of the employee questionnaire.

Exploring the attitudes of academic employees will undoubtedly differ across various universities. The next phase of the study includes replicating this data collection at other universities, within the U.S. and internationally. We believe culture will dictate much of the opinions and attitudes concerning privacy; therefore, much consideration has gone into the selection of the next university to explore.

A document from the OECD (Organisation de Cooperation et de Developpement Economiques) Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy published comparative findings concerning international use of technology (July, 1998). The results indicate that the country having the highest computer penetration in the workplace is Finland. The study also reports Finland with the highest percentage of citizens having Internet access, followed by the United States. For this reason, we are collaborating with a university in Finland to extend our findings into an international domain. The impact of this international study is expected to be valuable as universities continue expanding into the global education space with distance learning technologies.

6. References

- [1] D.Carnevale, "Education Department Proposes Guidelines for Changes in Law on Student Privacy", *The Chronicle of Higher Education*, June 11, 1999, p.A36.
- [2] CAUSE Report, "Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities", <http://www.educause.edu/pub/pubs.html>, 1999.
- [3] R.F.S.J.Curran, "Student Privacy in the Electronicera: Legal Perspectives", *CAUSE/EFFECT*, 12, 1989, pp.14-18.
- [4] J.B.Earp and F.C. Payton, "Information Privacy Concerns Facing Health Care Organizations in the New Millennium", Under Review at *ISR*, 2000.
- [5] W.H.Honan, "Education Department Sues Universities Over Disclosure of Crime Records", *New York Times*, February 4, 1998, p.14.
- [6] NACADA, "NACADA Mission Statement", <http://www.ksu.edu/nacada/>, 1999.
- [7] H.J.Smith, S.J. Milberg and S.J. Burke, "Information Privacy: Measuring Individuals' Concerns About Organizational Practices", *MIS Quarterly*, June 1996, pp 167-196.
- [8] C.B.Weiser, "Who's Wandering the Hallowed Halls?", *Security Management*, Aug. 1999, v43, i8, pp.57-62.
- [9] M.Weiser, "The Future of Ubiquitous Computing on Campus, Communications of the ACM", Jan. 1998, v.41, i.1, pp.41-42.
- [10] E.L.Yates, "The Lack of Virtual Privacy", *Black Issues in Higher Education*, Feb. 18, 1999, p.50.

Appendix

Survey Instrument - Adapted from Smith, et al. (1996)

- A. It usually bothers me when THE UNIVERSITY asks for student information.
- B. All the student information in computer databases should be double-checked for accuracy – no matter how much this costs.
- C. THE UNIVERSITY should not use student information for any purpose unless it has been authorized by the student who provided the information.
- D. THE UNIVERSITY should devote more time and effort to preventing unauthorized access to personal information.
- E. When THE UNIVERSITY asks students for personal information, I sometimes think twice before recording it.
- F. THE UNIVERSITY should take more steps to make sure that the student information in its files is accurate.
- G. When students give personal information to THE UNIVERSITY for some reason, THE UNIVERSITY should never use the information for any other reason (other than the original intention of assisting the student).
- H. THE UNIVERSITY should have better procedures to correct errors in student information.
- I. Computer databases that contain student information should be protected from unauthorized access – no matter how much it costs.
- J. It bothers me to give student information to other organizations.
- K. THE UNIVERSITY should never sell the student information in its computer databases to other companies.
- L. THE UNIVERSITY should devote more time and effort to verifying the accuracy of the student information in its databases.
- M. THE UNIVERSITY should never share student information with other companies unless it has been authorized by the students who provided the information.
- N. THE UNIVERSITY should take more steps to make sure that unauthorized people cannot access student information in its computers.
- O. I'm concerned that THE UNIVERSITY is collecting too much information about students.

NOTE: Each item is placed on a 7-point Likert scale anchored by "Strongly Disagree" (1) and "Strongly Agree" (7). Some items were modified due to the context of this research.