Monitoring of Electronic Communications at Universities: Policies and Perceptions of Privacy

Stan Kurkovsky
Central Connecticut State University
kurkovskysta@ccsu.edu

Ewa Syta
Central Connecticut State University
sytaewa@ccsu.edu

Abstract

This paper presents the results of a research study on the use of electronic communications by college students at public universities. We examine student perceptions and attitudes towards electronic communications, such as email, web browsing, using social networks, and other online activities, as well as their views and expectations of privacy and trust. We discuss a number of important characteristics of information technology as a facilitator of electronic communications on campus and their impact on the perceived privacy. We paid special attention to the effects of institutional policies concerning the monitoring of electronic communications and the resulting possible loss of privacy and trust. The results of our study indicate that regardless of their awareness of such policies, individuals have an inherent expectation that their on-campus electronic communications will stay private. Our results also suggest that average users do not understand the implications of electronic monitoring policies on their privacy. However, as a result of their understanding of these policies, users often adjust their communications in response to the possibility of diminishing privacy.

1. Introduction

Email has long been considered an important method to conduct unstructured communications, be it among employees of a company or faculty, staff, and students on a university campus. Email and other forms of electronic communications have been credited with increasing innovation, facilitating collaboration, and helping maintain social ties among people [52]. Over the last decade, many branches of government, businesses, and universities began adopting policies which effectively make email the preferred and official means of communication, making it equal to written (paper) communications in all respects. In this paper, electronic communications refer to email, instant messaging, web browsing, and other services involving transmission of electronic information.

In government and business environments, email and other forms of electronic communications are also viewed as a source of some adverse effects, such as an increase in the unproductive use of time and added security threats. In a corporate or government environment, it is clearly desirable that employees use these tools in a way that does not contradict managerial objectives [1]. However, if the organization strives to increase unstructured communication as a way to increase productivity and motivation, using such tools for private communications should be encouraged. On the other hand, if an organization considers email and other electronic communications media strictly as a means of efficient work-related communications, well-articulated policies need to be in place. The growth of email use has been followed rather than preceded by the adoption of policies as employers are trying to play catch up with the broadening use of electronic communication by employees.

There are many similarities between the use of electronic communications in academic and government or corporate environments. First of all, universities are businesses in the field of higher education. By their very definition, public universities are supported by state governments and operate within the context of existing state and federal laws and policies. As a result, all aspects of electronic communications occurring at or facilitated by public universities must be viewed in a broader context of the e-government domain. Although they may not have many trade secrets that need to be guarded from unauthorized discussion in email or other electronic media, universities are entrusted with a plethora of private student information containing their academic, financial, and health-related records. Policies concerning email use by university faculty and staff, therefore, could be quite similar to those adopted by business management or e-government. On the other hand, a typical information technology (IT) infrastructure on a university campus serves not only faculty and staff, but also a large student body. The amount of email and network traffic generated by students frequently and by a large measure exceeds that generated by faculty and staff. Student use of

electronic communications (including email, web browsing, and participation in social networks) could be very difficult to regulate. However, students by their very nature are more inclined to use these tools for purposes that are not related to their studies. Consequently, there is a clear need for university administrators to establish a set of policies that would regulate campus-wide use of electronic communications.

2. Private Information on Campus

Information systems of a typical public university may contain a substantial amount of personal information concerning students, faculty and staff. This information may include academic information such as grades, information about disciplinary actions, medical records, social security numbers, pay rates and annual salaries, etc. Until recently, few academic users were concerned about the privacy of their records in spite of having little knowledge of the details about how their records are acquired, processed and stored [28]. However, many recent reports of data theft and unauthorized access of university records have raised awareness of these issues [45]. Because IT departments are responsible for preventing such occurrences, it is natural for them to give a higher priority to the monitoring of network traffic and electronic communications over the privacy concerns of individual users [17]. Consequently, user privacy could be reduced to unacceptable levels. To prevent this, users should be made aware of the existing monitoring policies, as well as the specific techniques used to enforce compliance with such policies. Open and clear information about such policies is a step to build the trust of users and potentially reduce their concerns of diminished privacy [24,54].

One of the goals of the Family Educational Right to Privacy Act of 1974 (FERPA) is to protect student record privacy; it allows students to inspect the records pertaining to their academic activities, as well as limit their disclosure. However, there are many concerns of the effectiveness of this law in the days of ubiquitous electronic records and widespread network connectivity. A set of new interpretations came into effect in January 2009, but they were primarily a response to the 2007 Virginia Tech massacre and were mainly concerned with the use of student identification numbers and the release of student records. EDUCAUSE, a nonprofit association aimed to advance higher education by promoting the intelligent use of IT, maintains that FERPA is likely to be ineffective in protecting student privacy in the ever-evolving technological environment [18]. Main technological challenges to the privacy of student information identified by EDUCAUSE includes email, web browsing, digitized documents, digital signatures, audio and video conferencing, as well as electronic exchange, and the archiving and retrieval of student information.

3. Expectations of Privacy

Privacy, "the right to be left alone" [60] has been extensively analyzed from legal and philosophical points of view producing varying results. Most theorists take the view that privacy is a meaningful and valuable concept [14]; however, some argue that there is no right to privacy and that there is nothing special about privacy, because any interest defined as private are protected by rights to property and bodily security [55]. Although multiple definitions of and approaches towards privacy subsist, the term remains elusive as theorists try to define the scope and limits of privacy [22,39]. As the technology has advanced increasing the capabilities to gather, process, store and distribute all forms of information, the concept of privacy has become one of the most contentious issues of the information age [11]. Rapid growth of many Internet-enabled initiatives, such as e-government and on-line education, have led to new, more severe implications of privacy breaches, which have been attracting an ever-growing attention from the government, academia, and the public. A large body of relevant work on how users cope with privacy challenges of the digital world has shed some light on the subject [7,16,36,38,50]. College students, who are the study population of this paper, and different facets of their online habits and behavior, also have been intensely researched [8,41].

A body of existing research work indicates a number of possible reasons for the implicit expectation of privacy in electronic communications, which includes technological reasons, analogies with traditional postal mail, a feeling of security, and the absence of policy.

Misunderstanding of technology. In order to write an email or send a private message to another Facebook user, one needs to log in with a correct user name and password [10,61]. Such a login procedure may create an illusion of privacy that no one can read their email or private communication intended for another user. Furthermore, some users incorrectly assume that once email is delivered, no copies are left behind and when an email message is deleted all traces of its existence are irrevocably removed.

Postal mail analogy. Many users extend the expectations of privacy given to postal mail onto electronic mail [20]. Since it is illegal for anyone other than the addressee to open and read letters sent by

postal mail, many assume that the same analogy is true for email [49]. In fact, protections extended to postal mail under a number of federal laws do not extend to electronic mail or any other forms of electronic communications.

Feeling of security. A substantial amount of meaning in conversation is conveyed via nonverbal and emotional cues, which are absent in most electronic communication media (with the obvious exception of voice and video conference tools) [9,15]. Some research work suggests that reducing the presence of social context cues could lead to an increased feeling of security provided by a communication medium [20,61]. Email, discussion boards and social networking sites are among these kinds of media, and as a result, users often express themselves more openly under a misguided sense of privacy.

Absence of policy. If there are no explicit policies governing the use and monitoring of electronic communications, especially email, users may simply assume that all of their email is private [49].

In a business environment, the adoption of policies governing the electronic communications of employees may be an important tool serving many diverse purposes, such as guarding trade secrets [1], increasing productivity [10], and preventing any legal actions by employees against their employers [25,62]. Additionally, clearly specified policies could lead to improving employee morale and attitudes [33,40,43], as well as an increase in their trust of the employer [3,46,51].

A number of similar trends could be observed in an academic environment. However, two important factors must be taken into account that make an academic setting substantially different from a traditional business environment from the perspective of electronic communications monitoring. On the one hand, traditionally, faculty expect to enjoy the benefits of academic freedom, which entails the possibility of engaging in research in an extremely wide variety of subjects. As more and more sources of information (digital libraries, news agencies, etc.) are present online, more faculty members are accessing these resources. From the IT management perspective, it may be extremely difficult to distinguish from the content being accessed for personal reasons or for research purposes [32]. On the other hand, in a typical academic setting, students are responsible for generating a very substantial share of network traffic. While on campus, students could be using computers and the Internet connectivity during and outside of class time for both course-related activities and personal communication. Although it may be possible to establish and enforce an acceptable Internet use policy [23,48,53], students may not be aware of it and its implications.

The next section provides a sampling of acceptable Internet use policies from a broad spectrum of universities and analyzes their importance, and possible influence on the user behavior.

4. Campus Policies and Their Implications

As Internet access becomes an everyday necessity, many government offices, businesses, and institutions of higher education have established a range of formal acceptable use policies (AUP) regulating Internet access on their networks, as well as many forms of electronic communications. Many such policies include clauses explicitly indicating that the electronic communications occurring on the organization's network may and will be monitored [6]. In fact, a recent survey conducted by the American Management Association indicates that over 66% of al employers actively monitor electronic communications of their employees [4].

Ensuring policy compliance by users is a continued problem facing many organizations and their IT departments [47]. Organizations have to make a choice about how active they want to be in enforcing such policies. One option is access restriction, which may work well to block access to a list of well-known undesirable web sites or Internet services (this may also include complete access restriction to all external websites). However, in an academic environment such restrictive actions may be counterproductive given the varied range of users and the blurred boundaries between what may or may not be considered appropriate in an environment that is supposed to guarantee academic freedom. In circumstances when active policy enforcement may not be a viable option, organizations may choose to provide full access to all forms of electronic communications, but provide users with a fair warning [27]. Such warnings typically state the policies and consequences for failing to comply with these policies.

Current research indicates that users whose electronic communications may be monitored are more likely to comply with the corresponding monitoring policies if they are explicitly made aware of these policies and/or if they know that their communications are being observed [6]. Information systems for the monitoring of electronic communications have been shown to be an effective tool for detection and prevention of policy violations [5,21]. It is important to note that in many countries, including the European Union, it is illegal to use monitoring systems that violate employee privacy rights [37].

A substantial amount of current research indicates that when monitored, many individuals would adjust their communications in order to share less information and to reduce the volume of communications [2]. This could be explained by the desire of these individuals to present themselves in a kind of manner that they perceive to be more in line with what is expected from them by the monitoring authority [29,30]. In particular, some research work in the area of cognitive evaluation theory suggests that when individuals are monitored for control, e.g. for compliance with rules and policies, the intrinsic motivation of individuals is replaced with an extrinsic motivation of compliance with the expectations of the monitoring authority [19,35].

Many studies discovered evidence indicating that computer-based performance monitoring of user activities (including stress and health factors, satisfaction, work performance, etc.) could lead to an increase in the quantity of performance, but also to a decrease in work satisfaction, higher stress, as well as other adverse effects on the individuals being monitored [13,26,31]. This could be explained by the social facilitation theory, which suggests that in the presence of others people would perform better on easy tasks but worse on difficult tasks. However, this theory focuses mainly on highly structured tasks such as clerical work. Monitoring of typical electronic communications, such as email and web browsing, is much more complex and less structured [42,44].

Many universities have adopted a range of policies ranging from broad acceptable use policies to specific policies focusing on the monitoring of electronic communications [59]. For example, below is an excerpt from Acceptable Use of Computing Resources Policy adopted by the University of Florida [57]:

> *"While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service."*

Such a policy applies to all users of IT services provided by the university, including faculty, staff, students, and guests. This policy also makes it clear that all user activity may and will be logged. However, many users, especially students, may not be aware of the details of this seven page long policy. Furthermore, given the possibility that many of the users lack the necessary technological background, they may not fully understand the implications of this policy. For example, some users may assume that only login activities are recorded, while in fact this policy could be implemented to record all HTTP requests made from every computer on campus. At the same time, some universities choose to explain the specific rationale for such a policy and provide more details about the nature of records that will be kept. An Online Privacy Statement from the University of Minnesota explains that "there are four types of information that this site may collect during your visit: network traffic logs, web visit logs, cookies, and information voluntarily provided by you" [58].

The same policy from the University of Florida [57] goes further to provide for not only logging, but also for full-scale monitoring of all activities of individual users without their knowledge:

> *"The university may also specifically monitor the activity and accounts of individual users of university computing resources, including individual login sessions and the content of individual communications, without notice."*

The implementation of this policy could be completely justified from many points of view, including federal policy compliance, litigation support, service quality assurance, etc. However, those users who may have only a superficial exposure to policy compliance, especially students, may perceive such a policy as a substantial invasion of their privacy.

Many policies contain a vague statement that individual usage may be monitored. However, some universities, e.g., the City University of New York [12], in an attempt to lower the perceived intrusiveness of policies, explicitly state that individual usage of computer resources is not monitored, inspected, or disclosed without the user's consent, unless circumstances necessitate otherwise. The circumstances under which such information can be gathered without notice are clearly specified (in brief, to preserve the integrity, security, or functionality of computer resources, to ensure safety of users, and whenever required by law) as well as a protocol that has to be followed in such cases.

Many AUPs specifically indicate that there is a chance that university users may completely lose the privacy of their electronic documents and records. For example, below is an excerpt from Acceptable Use of Information Technology Resources chapter of the Operations Manual from the University of Iowa [57]:

> *"…users should be aware that their right to privacy in electronic records may be subject to the University's obligation to respond to subpoenas or other court orders, reasonable discovery requests, and requests for documents.* […] *Although it is the University's position that personal electronic files of faculty, staff, and students are not ordinarily to be considered 'public records,' users should be aware that a court of law, and not University officials, may ultimately decide such issues."*

Other universities (e.g. University of California Hastings College of the Law [56]) go one step further and openly state that while they will make every effort to respect the privacy on an individual's files and emails, there is absolutely no guarantee of privacy and/or confidentiality:

"...you should be aware that there is no guarantee of privacy or confidentiality with regard to email/Internet communications."

In general, acceptable use policies are intended to serve as guidelines for proper usage, but not as user controls. At the same time, according to a survey of AUPs used at a broad range of organizations (including institutions of higher education), many are not composed formally enough and are not sound from legal point of view [48]. However, they establish general rules for using computer resources that all users are assumed to follow, as well as a framework for understanding potential consequences which such usage may engender.

5. Research Hypotheses and Methodology

In order to study and analyze the effects of monitoring and acceptable use policies on electronic communications on public university campuses, we formulated a number of hypotheses reflecting students' perceptions and attitudes.

H1. Regardless or monitoring policies, users have an expectation of privacy in their electronic communications.

H1a. Understanding electronic monitoring policies and their effects on user privacy requires advanced knowledge, e.g., studying the implications of computing on society.

H2. Electronic monitoring policies help users understand the difference between electronic communications at home and on campus.

H3. Publicizing electronic monitoring policies helps increase user trust.

H4. As a result of monitoring policy enforcement, users will consciously limit or adjust their electronic communications.

We expect that the presence of, and knowledge and/or awareness of, electronic monitoring policies will have a profound effect on the way students use electronic communications media. We also expect that there will be a substantial difference in students' attitudes regarding electronic monitoring based on the depth of their understanding of the social implications of computing and technology. In the following sections, we describe the research study and analyze the obtained results.

The study was conducted in April 2010. Participation in the study was voluntary, survey responses were anonymous, and participants were not compensated. Sixty-five students, ages 18-25, from three different undergraduate courses were recruited for this study and divided into three groups based on the course from which they were recruited. Groups labeled C and E1 were recruited from several general education courses that emphasized introductory computer programming and web design skills. These groups consisted of students majoring in a broad range of disciplines that excluded computer science and information technology. The group labeled E2 was recruited from a senior-level non-technical computer science course focusing on the legal, social, ethical, and economic issues of IT. Approximately one half of this group consisted of computer science students; the rest of the students majored in information technology, design, and engineering disciplines. Characteristics of the study participants are summarized in Table 1. On average, each student was using a computer just over 5 hours a day, with at least half of that time actively using the Internet. Also, an average study participant has been using computers for over eleven years. Such data suggests that the students participating in this study were appropriate for the research objectives.

Table 1. Characteristics of the study participants

Variable	Mean	StDev
Hours using a computer each day	5.05	3.04
Hours using a computer on campus each day	2.12	1.96
Hours accessing the Internet	2.59	3.08
Years using computers	11.32	3.20

Members of all groups were asked to complete a survey consisting of series of questions aimed to measure their attitudes about privacy of their electronic communications on campus as well as their perception of being monitored. As shown in the Appendix, our survey instrument offered to all members of the group incorporated four constructs measuring their perception of privacy while using campus computers for electronic communications, trust to the university regarding privacy of information, the effects of electronic communication policy enforcement on their computer use, and comparing their computer use and electronic communications while at home to that on campus. Answers to all questions were based on a standard 7-point Likert scale anchored by 'Strongly agree' (1) and 'Strongly disagree' (7).

Group C was chosen as a control group (n=20). Members of this group were not provided with any additional information regarding electronic communications monitoring policies currently in place on campus. It was expected, however, that members of

all groups would have some awareness of such policies because all students are presented with a text of this policy when university email accounts are created for them. Additionally, all desktop computers on campus present users with a corresponding message at login.

Groups E1 and E2 served as experimental groups. Groups E1 (n=19) and E2 (n=26) were presented with the text of the current policy for electronic communications monitoring immediately before they were asked to complete the survey. It was expected that members of the group E2 would have a substantially better understanding of the implications of this policy because of the subject matter they studied in the course from which they were recruited.

For the purposes of this study, groups C and E1 represent average users who do not possess any in-depth technical background. Group E2, however, represents somewhat more advanced users who possess a substantially better understanding of social implications of computing technology.

Table 2. Descriptive statistics

Characteristics	Group C		Group E1		Group E2	
	Mean	StDev	Mean	StDev	Mean	StDev
PRIVACY1	5.90	1.65	5.11	1.85	3.54	2.32
PRIVACY2	5.80	1.91	5.05	1.99	3.50	2.06
PRIVACY3R	5.80	1.85	4.89	1.56	4.46	2.06
PRIVACY4R	5.05	1.64	4.32	1.49	3.81	2.14
HOME1	2.75	1.65	4.32	1.29	4.19	2.21
HOME2	2.95	1.67	4.05	1.39	3.96	2.22
TRUST1	3.30	1.45	4.32	1.16	2.85	1.49
TRUST2	3.15	1.35	3.79	1.55	2.65	1.41
TRUST3	3.60	1.14	4.16	1.01	3.04	1.54
ENFORCEMENT1	4.15	1.98	4.05	1.31	2.62	1.70
ENFORCEMENT2R	4.80	2.04	4.11	1.88	2.69	2.07
ENFORCEMENT3	5.30	2.08	4.00	1.70	3.77	2.35
N	**20**		**19**		**26**	

6. Analysis and Findings

Table 2 shows descriptive statistics for all individual components of every research construct used in this study. The validity of these measures was established using a factor analysis procedure whose results are summarized in Table 3. Principal component factor analysis yielded four factors whose Eigen values were greater than 1 and which collectively accounted for 75.36% of the variance.

A series of ANOVAs on every characteristic was performed on each of the study groups. Results are presented in Table 4.

Hypothesis H1 proposed that the users have an inherent expectation of the privacy of their electronic communications regardless of whether monitoring policies are in place. There is no statistical difference between control and experimental group E1 (p=0.1652, p=0.2383, p=0.1081, p=0.1525). Subjects in both groups indicated that they generally expect their emails and web browsing to be private and viewed electronic monitoring policy in effect on campus as a direct threat to their privacy. Therefore, our findings provide H1 with full support.

Table 3. Results of factor analysis

Characteristics	F1	F2	F3	F4
TRUST1	0.827			
TRUST2	0.776			
TRUST3	0.744			
PRIVACY4R		0.908		
PRIVACY1		0.784		
PRIVACY2		0.777		
PRIVACY3R		0.777		
ENFORCEMENT3			0.665	
ENFORCEMENT1			0.433	
ENFORCEMENT2R			0.405	
HOME2				0.609
HOME1				0.577
Eigen value	5.57	4.38	2.52	1.10
Variance (%)	30.95	24.31	13.98	6.12

Hypothesis H1a proposed that users should have advanced knowledge in order to understand the effects of electronic monitoring policies on their privacy. Members of group E2 have gained such knowledge in the course on social issues in computing from which they were recruited. As shown by our findings supporting hypothesis H1, typical users expect privacy in their communications whether or not they were

made aware of the monitoring policy. On the contrary, members of group E2 indicated that they do expect their privacy to be limited as a result of the policy. The difference in responses between control and experimental groups are statistically significant (p=0.0004, p=0.0004, p=0.0276, p=0.0365), which provides hypothesis H1a with full support.

Table 4. Statistical analysis of survey results

Constructs and their characteristics	p-values	
	Group E1	Group E2
Privacy and perception of threats to privacy		
PRIVACY1	0.1652	0.0004
PRIVACY2	0.2383	0.0004
PRIVACY3R	0.1081	0.0276
PRIVACY4R	0.1525	0.0365
Home vs. campus use of computers for electronic communications		
HOME1	0.0022	0.0188
HOME2	0.0317	0.0960
Trust in privacy protection		
TRUST1	0.0213	0.3062
TRUST2	0.1767	0.2349
TRUST3	0.1161	0.1781
Effects of policy enforcement		
ENFORCEMENT1	0.8581	0.0071
ENFORCEMENT2R	0.2771	0.0013
ENFORCEMENT3	0.0398	0.0264

Hypothesis H2 proposed that electronic monitoring policies help users understand the difference between electronic communications at home and on campus. Compared to the control group, subjects who were made aware of these policies generally were much less inclined to equate electronic communications at home and on campus. Based on our findings, this hypothesis has full support based on the responses of typical users (E1, p=0.0022, p=0.0317) and partial support based on the responses of advanced users (E2, p=0.0188, p=0.0960). Group E2 gave a response to the HOME2 question that was not statistically different from the control group. In this question both groups agreed that they feel equally easy about using Facebook while on campus and while at home. This could be explained by the fact that the members of the advanced group have a good understanding of the general lack of privacy protection on Facebook, regardless whether it is used on campus or at home.

Hypothesis H3 proposed that making users aware of electronic monitoring policies helps increase their trust to the monitoring authority. Although the subjects from all groups indicated a very moderate to neutral degree of trust to the monitoring of electronic communications, there was no statistically significant difference between the groups (p=0.2349, p=0.1161, p=0.1781, p=0.0213, p=0.3062, p=0.1767). Therefore, our findings fail to support hypothesis H3.

Hypothesis H4 proposed that as a result of enforcing monitoring policy, users will consciously limit or adjust their electronic communications. Subjects from the control group and experimental group E1 indicated that in general electronic monitoring policies and their enforcement have no effect on their use of campus computers, web browsing patterns or choosing what information to post on social networks. Overall, there was no statistically significant difference in their responses (p=0.8581, p=0.2771, p=0.0398). Consequently, our findings do not provide support for hypothesis H4 among the group of typical users. However, subjects from the experimental group E2 indicated that the enforcement of these policies does have a profound impact on their electronic communications while on campus; these results were statistically different from the control group (p=0.0071, p=0.0013, p=0.0264). These results provide support for hypothesis H4 among the advanced user group, which echoes our findings for hypothesis H1a discussed above.

7. Discussion and Conclusion

Our results show that in general, individuals expect that their electronic communications will remain private regardless of the implications of electronic monitoring policies or their knowledge and/or awareness of such policies. Furthermore, users often feel that there is no difference in the way they can use home and campus computers for communications. However, individuals who possess a more in-depth knowledge of general implications of computing on society seem to be open to the idea that their electronic communications on campus may not be entirely private. Our findings also suggest that regardless of their knowledge or policy awareness, individuals tend to be rather neutral in trusting that their privacy and that of their records is protected by the university and its IT infrastructure.

Our findings suggest that average users lack any significant understanding of acceptable use and electronic monitoring policies. Although electronic monitoring was present and users were made aware of the corresponding policies, this had no significant effect on their communication patterns and preferences. However, individuals with a deeper understanding of the implications of such policies reportedly adjusted their communications in response to the resulting possibility of diminishing privacy.

These findings may have significant implications for the application of electronic monitoring policies in

an academic setting and elsewhere. Users need to be better educated about what such policies might entail in a manner that is accessible to them. Although these policies may be clearly written and appear unambiguous to staff, administrators and IT personnel, they seem to be falling on deaf ears when it comes to the largest group of users – students.

This study focused on 'the big picture' of student perception, attitudes, and behavior in the context of electronic communications monitoring. It may be worthwhile to extend this research to look at different ways in which such policies could be written in order to maximize student comprehension of these policies.

Student attitudes and perceptions of privacy in light of electronic policies will undoubtedly vary at different institutions. Another direction for future work could extend this study longitudinally and replicate it across other universities. It will be especially interesting to study student attitudes and opinions about privacy internationally, and particularly in the European Union, where privacy laws are substantially different from those of the United States.

8. References

[1] Agarwal, R., Rodhain, F., "Mine or Ours: Email Privacy Expectations, Employee Attitudes, and Perceived Work Environment Characteristics," In Proc. *35th Annual Hawaii International Conference on Systems Sciences*, Hawaii, 2002.

[2] Aiello, J., "Electronic Surveillance and Its Effects," *Journal of Applied Social Psychology*, 1993, 23(7): 499-507.

[3] Alder, G., Noel, T, Ambrose M., "Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust," *Information & Management*, 2006, 43(7): 894-903.

[4] American Management Association, *Electronic Monitoring and Surveillance 2007 Survey*. February 2008, retrieved from http://www.amanet.org/training/whitepapers/2007-Electronic-Monitoring-and-Surveillance-Survey-41.aspx

[5] Antoniou, G., Parampalli, U., Batten, L., "Monitoring Employees' Emails without Violating Their Privacy Right," In Proc. *8th International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2007, pp. 46-50.

[6] Arnesen, D., Weis, W., "Developing an Effective Company Policy for Employee Internet and Email Use." *Journal of Organizational Culture, Communications and Conflict*, 2007, 11(2): 53-66.

[7] Bellman, S., Johnson, E., Kobrin, S., Lohse, G., "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society: An International Journal*, 2004, 20(5):313-324.

[8] Boyd, D., "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life," In *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media* Volume, D. Buckingham, ed., MIT Press, 2007, pp. 119-142.

[9] Byron, K., Baldridge, D., "E-Mail Recipients' Impressions of Senders' Likability: The Interactive Effect of Nonverbal Cues and Recipients' Personality," *Journal of Business Communication*, 2007, 44(2):137-160.

[10] Cappel, J., "Closing the E-Mail Privacy Gap," *Journal of Systems Management*, 1993, 44(12):6-11.

[11] Clarke, R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 2006, retrieved from http://www.rogerclarke.com/DV/Intro.html

[12] The City University of New York, "*Policy on Acceptable Use of Computer Resources,*" retrieved from http://portal.cuny.edu/cms/id/cuny/documents/level_3_page/001171.htm

[13] Corea, S., "Mounting effective IT based customer service operations under emergent conditions: Deconstructing myth as a basis of understanding," *Information and Organization*, 2006, 16(2): 109-142.

[14] DeCew, J., *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997.

[15] Derks, D., Bos, A., von Grumbkow, J., "Emoticons and Social Interaction on the Internet: the Importance of Social Context," *Computers in Human Behavior*, 2007, 23(1): 842-849.

[16] Dinev, T., Hart, P., "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce*, 2006, 10(2): 7-31.

[17] Earp, J. Payton, F., "Data Protection in the University Setting: Employee Perceptions of Student Privacy," In Proc. *34th Hawaii International Conference on System Sciences*, 2001.

[18] EDUCAUSE, "Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities", *CAUSE Report*, 1997, retrieved from http://net.educause.edu/ir/library/pdf/PUB3102.pdf.

[19] Enzle, M., Anderson, S., "Surveillant Intentions and Intrinsic Motivation," *Journal of Personality and Social Psychology*, 1993, 64: 257-266.

[20] Farrell, S., "Why Don't We Encrypt Our Email?" *IEEE Internet Computing*, 2009, 13(1): 82-85.

[21] Fleming, S., "Implicit Trust Can Lead to Data Loss," *Information Systems Security*, 2007, 16(2):109-113.

[22] Floridi, L., "Four Challenges for a Theory of Informational Privacy," *Ethics and Information Technology*, 2006, 8(3):109-119.

[23] Flowers, B., Rakes, G., "Analyses of Acceptable Use Policies Regarding the Internet in Selected K-12 Schools," *Journal of Research on Computing in Education*, 2000, 32(3):351-65.

[24] Frey, B., "Does Monitoring Increase Work Effort? The Rivalry With Trust And Loyalty," *Economic Inquiry*, 2007, 31(4):663-670.

[25] Friedman, B., Reed, L., "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use," *Employee Responsibilities and Rights*, 2007, 19(2):75-83.

[26] Grant, R. Higgins, C., "Computerized performance monitors as multidimensional systems: derivation and application," *ACM Transactions on Information Systems*, 1996, 14(2):212-235.

[27] Greenfield, D. Davis, R., "Lost in Cyberspace: the Web at Work." *CyberPsychology and Behavior*, 2002. Vol. 5, No. 4, pp. 347-353.

[28] Hole, K., Netland, L., Espelid, Y., Klingsheim, A., Helleseth, H., Henriksen, J. "Open Wireless Networks on University Campuses." *IEEE Security and Privacy*, 2008, 6(4):14-20.

[29] Holton, C., Fuller, R., "The Impact of Electronic Monitoring on Hazard Communications," In Proc. *39th Hawaii International Conference on System Sciences*, 2006.

[30] Holton, C. Fuller, R., "Unintended Consequences of Electronic Monitoring of Instant Messaging," *IEEE Transactions on Professional Communication*, 2008, 51(4):381-395.

[31] Irving, R., Higgins, C., Safayeni, F., "Computerized Performance Monitoring Systems: Use and Abuse," *Communications of the ACM*, 1986. Vol. 29, No. 8, pp. 794-801.

[32] Johnson, J. Chalmers, K., "Identifying Employee Internet Abuse," In Proc. *40th Hawaii International Conference on System Sciences*, 2007.

[33] Johnson, J., Ugray, Z., "Employee Internet Abuse: Policy Versus Reality," *Issues in Information Systems*, 2007, Vol. VIII, No. 2, pp. 214-219.

[34] Kato, Y., Kato, S., Akahori, K., "Effects of Emotional Cues Transmitted in E-mail Communication on the Emotions Experienced by Senders and Receivers," *Computers in Human Behavior*, 2007, 23(4):1894-1905.

[35] Martens, R., Gulikers, J., Bastiaens, T., "The impact of intrinsic motivation on e-learning in authentic computer tasks," *Journal of Computer Assisted Learning*, 2004, 20(5):368-376.

[36] Meinert D., Peterson D., Criswell J., Crossland M., "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," *Journal of Electronic Commerce in Organizations*, 2006, 4(1):1-17.

[37] Mitrou, L., Karyda, M., "Employees' Privacy vs. Employers' Security: Can They Be Balanced?" *Telematics and Informatics*, 2006, 23(3):164-178.

[38] Nehf, J., "Shopping for Privacy on the Internet," *Journal of Consumer Affairs*, 2007, 41(2):351-365.

[39] Nissenbaum, H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy*, 1998, 17:559-596.

[40] Oravec, J., "Constructive Approaches to Internet Recreation in the Workplace," *Communications of the ACM*, 2002, 45(1):60-63.

[41] Palfrey, J., Gasser, U., *Born Digital*, New York: Basic Books, 2008.

[42] Papanikolaou, K., Grigoriadou, M., Magoulas, G., Kornilakis, H., "Towards new forms of knowledge communication: the adaptive dimension of a web-based learning environment," *Computers & Education*, 2002, 39(4):333-360.

[43] Paschal, J., Stone, D., Stone-Romero, E., "Effects of Electronic Mail Policies on Invasiveness and Fairness," *Journal of Managerial Psychology*, 2009, 24(6):502-525.

[44] Peters, L., "Conceptualising computer-mediated communication technology and its use in organisations," *International Journal of Information Management*, 2006, 26(2):142-152.

[45] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, 2010, retrieved from http://www.privacyrights.org/ar/ChronDataBreaches.htm

[46] Raghupathi, W., "Corporate Governance of IT: a Framework for Development," *Communications of the ACM*, 2007, 50(8):94-99.

[47] Saran, M., Zavarsky, P., "A Study of the Methods for Improving Internet Usage Policy Compliance," In Proc. 2009 *IEEE International Conference on Computational Science and Engineering*, pp. 371-378.

[48] Siau, K., Nah, F., Teng, L., "Acceptable Internet Use Policy," *Communications of the ACM*, 2002, 45(1):75-79.

[49] Sipior, J., Ward, B., "A Framework for Employee E-mail Privacy Within the United States", *Journal of Internet Commerce*, 2009, 8(3):161-179.

[50] Smith, H., Milberg, S., Burke, S., "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, 1996, 20(2):167-196.

[51] Snyder, J., Cornetto, K., "Employee Perceptions of E-mail Monitoring from a Boundary Management Perspective," *Communication Studies*, 2009, 60(5):476-492.

[52] Sproull, L., Kiesler, S., "Reducing Social Context Cues: Electronic Mail in Organizational Communication", *Management Science*, Institute for Operations Research and the Management Sciences, 1986, 32(11):1492-1512.

[53] Stewart, F., "Internet Acceptable Use Policies: Navigating the Management, Legal, and Technical Issues" *Information Systems Security*, 2000, 9(3):1-7.

[54] Tabak, F., "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development," *Employee Responsibilities and Rights Journal*, 2005, 17(3):173-189.

[55] Thomson, J., "The Right to Privacy", *Philosophy and Public Affairs*, 1975, 4: 295-314.

[56] University of California Hastings College of the Law, "*Acceptable Use Policy*," retrieved from http://www.uchastings.edu/check-email.html

[57] University of Florida, "*Acceptable Use of Computing Resources Policy*," retrieved from http://www.it.ufl.edu/policies/aupolicy.html

[58] University of Minnesota, "Online Privacy Statement," retrieved from http://www.privacy.umn.edu/

[59] Wada, K., "The Right to Be Let Alone," EDUCAUSE Review, 2010, 45(1):56-57.

[60] Warren, S., Brandeis, L., "The Right to Privacy", *Harvard Law Review*, 1890, IV(5):193-220.

[61] Weisband, S., Reinig, B., "Managing User Perceptions of Email Privacy," *Communications of the ACM*, 1995, 38(12):40-47.

[62] Wright, B., "E-Mail Discovery: Latest Cases Impel Public Agencies to Retain Records," *EDPACS*, 2010, 41(3):8-13.

Appendix
Research constructs and questions

Privacy and perception of threats to privacy
PRIVACY1. Regardless of the law, I believe that the university officials have the right to observe my electronic communications (e.g. sending/receiving email, posting messages on Facebook, visiting websites)
PRIVACY2. When I send email, I typically do not have an expectation of privacy
PRIVACY3. Any email I send is exclusively my property
PRIVACY4. I feel that campus Electronic Monitoring Policy violates my privacy

Effects of policy enforcement
ENFORCEMENT1. Electronic Monitoring Policy has a significant effect on how I use computers on campus
ENFORCEMENT2. Electronic Monitoring Policy does not influence the choice of websites I visit
ENFORCEMENT3. Electronic Monitoring Policy makes me think about what I post on Facebook

Home vs. campus use of computers for electronic communications
HOME1. I feel equally easy about emailing my friends while on campus and while at home
HOME2. I feel equally easy about using Facebook while on campus and while at home

Trust in privacy protection
TRUST1. I believe that the University makes the best decisions concerning information privacy
TRUST2. Overall, I trust the information security and privacy protection provided by the University
TRUST3. The University is doing the best job of making sure that my private information stays private