

# KNOWLEDGE OF PRIVACY, PERSONAL USE, AND ADMINISTRATIVE OVERSIGHT OF OFFICE COMPUTERS AND E-MAIL IN THE WORKPLACE

THOMAS W. DILLON

DAPHYNE S. THOMAS

*The objective of this research is to investigate the general public's attitudes and knowledge of the accessibility, personal use, and administrative oversight of office computers and e-mail. Survey data from over 1,000 respondents were collected and statistically analyzed. Those with higher incomes, higher levels of education, and those working for larger and more formal organizations have greater understanding of the accessibility and use of e-mail and office computers. Younger males with higher education and incomes report using office e-mail and computers most often for personal use. Additionally, employees working in government are more likely to be aware of administrative oversight of employee computer files and e-mail. Findings indicate employers should take steps to enhance employee knowledge concerning office computer and e-mail privacy issues, performance monitoring, and employer surveillance.*

Use of computers and e-mail has increased dramatically in the past 20 years. The increase in usage has magnified the importance of technology in business and the need for proper managerial oversight of technology. To provide this oversight employers frequently engage in e-mail monitoring, instant message monitoring, phone monitoring, and keystroke logging. The reasons for employer invasion of personal privacy of e-mail or office computers often involve issues such as security risks, preventing sexual harassment, and ensuring the acceptable performance of employees (Alderman & Kennedy, 1995). Invasive employer protective measures are often balanced with the possible risk of diminishing employee morale and dignity, and increasing worker stress.

Technological advances such as e-mail and the Internet are designed to make the workplace more efficient. These tools also expose employers to new types of employment law claims, including e-harassment. There are three main reasons employers monitor employees: legal liability issues, employee productivity, and security breaches (Crane, 2005). Some employers may decide to monitor the use of e-mail and the Internet to limit their exposure to discrimination and/or harassment claims (Kelly, McHenka, & Zielinski, 1999). In addition, employers also are

concerned about employees sharing, intentionally or inadvertently, the company's trade secrets and other proprietary or confidential information with competitors.

In spite of growing scrutiny from courts and regulators, it is reported that most employers are doing a poor job of managing e-mail business records and preparing for the likelihood of e-mail discovery (Flynn & Majerus, 2003). Consequently, employers are seeking new ways to address these concerns, including employee surveillance software. Surveillance software sales are estimated at \$140 million a year, and new technological advances provide employers with a number of options in monitoring devices (Flynn & Majerus). These software monitoring devices may include keystroke counters, image and picture inspectors, or select interval screen shot image reviewers. (Flynn & Majerus).

*Thomas Dillon is Professor, Computer Information Systems & Management Science, College of Business, James Madison University, Harrisonburg, Virginia.*

*Daphyne Thomas is Adolph Coors Business Professor, Finance & Business Law, College of Business, James Madison University, Harrisonburg, Virginia.*

In order to understand employee knowledge of e-mail and office computer privacy better, specifically issues created by employer monitoring and oversight, we surveyed over 1,000 people who were currently working or who worked within the past year. Our survey questions focused on e-mail and office computer privacy.

## BACKGROUND

### *E-MAIL PRIVACY*

Research shows that the average employee spends 25% of the workday on e-mail, with 8% of workers devoting over 4 hours a day to e-mail activities (Henderson & Snyder, 1999). Considering this ever-increasing emphasis on workplace e-mail use, it is not unrealistic that many employers institute rules, policies, and procedures for e-mail use and institute monitoring practices that may invade employee privacy (Kovach, Jordan, Tansey, & Framinan, 2000; White & Pearson, 2001).

Findings from a publication by the ePolicy Institute and Clearswift reveal that 62% of employers monitor employees' e-mail and Internet use and that most employers (68%) who monitor e-mail and Internet use cite legal liability as the primary reason to monitor (Flynn & Majerus, 2003). Only 10% of the companies responding to their survey have been ordered by courts to turn over employee e-mail related to workplace lawsuits. Sexual harassment and/or sexual discrimination claims stemming from employee e-mail and/or Internet use have affected 8.3% of the responding organizations.

The ePolicy Institute (Kelleher & Flynn, 2003) reports that employers fail to educate employees about e-mail risks, rules, and responsibilities. Kelleher and Flynn's findings show that 75% of organizations have written e-mail policies in place; however, only 48% offer e-mail policy education to employees, and only 27% offer e-mail record retention training.

The ePolicy Institute (Kelleher & Flynn, 2003) also reports that 90% of employers have installed software to monitor incoming and outgoing e-mail, but only 19% are using technology to monitor internal e-mail among

employees. This management failure to check internal e-mail is a potentially costly oversight. Casual e-mail conversations between employees are the type of messages that tend to trigger lawsuits, arm prosecutors with damaging evidence, and provide the media with embarrassing real-life disaster stories. Kelleher and Flynn also report that 90% of respondents send and receive personal e-mail at work and that 66% of companies lack a policy for deleting nonessential messages.

If the employer has a no privacy workplace communications policy, employees are on notice that their communications are being monitored, and courts generally find that employees lack an expectation of privacy in workplace communications (*Muick v. Glenayre Electronics*, 7th Cir. 2002). Sometimes courts look to whether an employee has specifically signed a policy agreeing to electronic monitoring or whether the electronic mail system provides a written notice each time the employee logs into the system (*Fraser v. Nationwide Mutual Insurance Co.*, E.D. Pa. 2001).

There is very little empirical research examining employee perceptions of e-mail monitoring by an employer. In a survey on software ownership, privacy, and workplace monitoring, Loch, Conger, and Oz (1998) found that respondents expressed strong agreement that using company e-mail for personal reasons was ethical, even if employer policies restricted use. Loch and her colleagues also reported that employer monitoring of e-mail was viewed as unethical behavior. These findings reflected similar results for telephone conversations.

In an early controlled study of ethical beliefs and perceptions of e-mail privacy, Cappel (1995) reported that there is significant resistance to e-mail monitoring. Most individuals surveyed had a poor understanding of personal e-mail rights. Cappel recommended that organizations needed to develop and promote e-mail policies better.

Not surprisingly, a survey of information system managers reported that 100% of respondents agreed that company rights took precedence over the privacy rights of the employee in relation to e-mail and Internet use (White & Pearson, 2001). Productivity

improvements and the avoidance of legal problems were the reasons given for preference over employee rights.

Hoffman, Hartman, and Rowe (2003) conducted a survey of company employees designed to discover the extent to which e-mail and Internet use is monitored. They found that monitoring is commonplace and performed regularly, even without given cause for concern.

In a multiple case study investigation of e-mail system monitoring and control in four companies, Duane and Finnegan (2004) found that there is a need to formulate a coordinated and comprehensive response consisting of technical, formal, and informal controls. They identify key factors, such as management committees, training, policies, and sustained awareness, for effectively monitoring e-mail and Internet usage (Duane & Finnegan, 2004).

#### *WORK/OFFICE COMPUTER PRIVACY*

The Electronic Privacy Information Center reports that in the workplace, of 115 million adults age 25 and over, 65 million, or 57%, use a computer at work. The percentage of employees using the Internet and/or e-mail at work increased from 18% in 1998 to 42% in 2001 (Electronic Privacy Information Center [EPIC], 2003).

The Electronic Communications Privacy Act of 1986 (ECPA) is the only federal statute that offers protection for workers in office computer privacy (Kovach et al., 2000). ECPA prohibits the intentional interception of electronic communications. However, the ECPA contains two loopholes that facilitate the invasion of employee privacy for monitoring and performance purposes. First, employers are permitted to monitor networks for business purposes. This enables employers to listen in on employee phone calls, view employees' e-mail, and view available documents. Under federal law, employers may not monitor purely personal calls. To determine that a call is personal, an employer usually must listen to portions of the employee's conversation. Once an employer knows that a call is personal, the employer must immediately stop monitoring the call. Second, an employer may intercept communications where there is actual or implied

employee consent. Consent has been found where an employer merely gives notice of the monitoring (EPIC, 2003). Some states have laws that require employers to signal or indicate that someone is listening (Kovach et al., 2000).

In response to an ethics survey, Loch et al. (1998) found that respondents feel that employer monitoring of employees is unethical, unless the monitoring is of software that carries a licensing agreement from a vendor. They report that respondents believe that the use of standard business software, such as word processing software, for personal reasons is not considered a breach of ethical behavior by an employee. Respondents consider employers who monitor word processing to be participating in unethical behavior.

Corporations have profit as a motive to protect their companies from possible privacy problems. Corporations also have the resources to devote to greater security and surveillance (Henderson & Snyder, 1999). Lane (2003) reports that post 9/11 surveillance of e-mail and office computer use is much more acceptable, both in and out of the workplace. Surveillance has taken center stage with the world on heightened alert to terrorism, and the private sector has moved rapidly to adopt provisions allowing for more surveillance (Cockcroft, 2002; Stone, 2004).

Many companies face legislation that impacts the use of internal e-mail and Internet use. The Sarbanes-Oxley Act of 2002 extends the need for record retention to include e-mail related to financial audits (Pub. L. No. 107-204, 116 Stat. 745, 2002). The Gramm-Leach-Bliley Act of 1999 mandates the need to safeguard the security and privacy of nonpublic customer data; protect against virus infection, network failure, data corruption, and other reasonably anticipated threats; and protect the privacy of customer information transmitted across open networks (Pub. L. No. 106-102, 113 Stat. 1338, 1999). Employers also have an incentive to ensure that employees do not unwittingly or intentionally divulge company trade secrets and intellectual property by way of their communications (Smith, 2003). Furthermore, employers want to prevent or remedy any defamatory statements made by

employees in electronic and other communications. In a recent court ruling, Judge Diarmuid O'Scannlain noted in a 3-0 ruling that current social norms suggest that employees are not entitled to privacy when using workplace computers that belong to their employers. Misuse of computers by employees may pose significant dangers in diminished productivity and employer liability (Egelko, 2006).

## METHODOLOGY

In the *Privacy Rights Handbook*, Givens (1997) provides consumers with information about their rights as based in law, as well as the many gaps where there are no specific legal rights. Questions in our survey are derived from privacy issues and concerns identified in the *Handbook*. The survey we administered identifies e-mail and office computer privacy problems and seeks input from employees as to their knowledge and recognition of these privacy issues.

### RESEARCH OBJECTIVE

Even though employer monitoring of employee performance is not new, the introduction of office computers and e-mail have introduced practical and legal elements, including work privacy issues. Generally, the employer owns the computer network and the terminals, and he or she is free to monitor employees (Privacy Rights Clearinghouse, 2006). This survey research project measured the general public's attitudes and knowledge of e-mail and office computer privacy with an emphasis on accessibility, privacy, and security. Importance was placed on the collection of real world data from multiple business and organizational environments.

### DATA COLLECTION PROCEDURES

The data were collected in a recent survey of approximately 1,060 adults from the general public. Most respondents lived in the mid-Atlantic states of Virginia, Maryland, Pennsylvania, and New Jersey. To avoid the high nonresponse rate of typical mail surveys, the data were voluntarily collected by 106 uncompensated student

fieldworkers who each delivered and retrieved 10 self-administered questionnaires from fieldworker-selected locations such as shopping malls and neighborhoods. Students received a 2% participation grade for assisting with the research project. The self-administered questionnaire was completed anonymously and without compensation.

Student fieldworkers tend to select certain types of respondents, such as individuals of the same social class, age, and gender as the fieldworker, and those who appear more leisurely, friendly, or attractive. For this reason each fieldworker was assigned a flexible quota of 10 respondents in this convenience sample as described by Alreck and Settle (1995). To insure an adequate number of each demographic group, each fieldworker was required to gather data from five males and five females. One female and one male were to be between the ages of 22 and 29, one female and one male were to be between 30 and 39, and so on up to age 60 and over. But, since age is sometimes difficult to determine, flexibility was permitted.

The age of 22 was the designated lowest age to reduce the possibility of unemployed respondents. The size and nature of the multi-page survey instrument deterred the use of a random sample. The process was monitored closely and 5% of the responses were verified by telephone to insure reliability. Twelve surveys were unusable and discarded.

### SURVEY INSTRUMENTS

A cover letter solicited the respondents' cooperation and assured anonymity. The questionnaire took about 10 minutes to complete. Institutional review board procedures were followed.

The first section of the questionnaire was designed to capture demographic data pertaining to age, sex, family income, highest level of education, employment sector, and length of employment at the current employer.

The second section of the questionnaire was designed to capture the respondent's knowledge of e-mail and office computer privacy. It contained 11 statements directly related to e-mail

and office computer accessibility, privacy, and security. The scale was a 5-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. Six of the 11 statements were reversed and recoded to prevent response bias. All 11 questions are included in the Appendix.

The initial questions for the e-mail and office computer privacy survey were obtained from previous published works (Alderman & Kennedy, 1995). The privacy issues were then discussed with a focus group and modifications were made to the survey to reflect focus group feedback, timeliness, and to incorporate current privacy issues.

Reliability analysis was performed to identify the factors for the 11 items in the questionnaire. Content validity was tested with factor analysis using principal components method with varimax rotation. We found that 10 items loaded on three factors. Table 1 presents the e-mail and office computer items that loaded on each factor. One item, “computerized personnel files are strongly secured,” did not load on the common factors and was discarded. Instead of loading on two privacy constructs, one for e-mail and one for office computer use, the 10 items loaded on three privacy factors that were shared by both. This is similar to findings by Hoffman et al., (2003) where most executives who responded to a survey saw no difference between e-mail and office

computer concerns. Factor 1 items can be identified as those privacy issues concerned with “accessibility and use of e-mail and office computers” (AU). Factor 2 items loaded on the privacy issue of “personal use of e-mail and office computer” (PU). Factor 3 items identified closely with “administrative oversight of e-mail and office computer” (AO).

Table 2 presents the Cronbach’s alpha for each multi-item factor. Factors 1 and 2 have acceptable reliabilities for exploratory analysis (Straub, 1989). Factor 3 has a low Cronbach’s alpha and should not be considered a fully reliable measure, but we will include Factor 3 in the discussion.

*RESEARCH QUESTIONS*

With the results of our reliability analysis, we slightly revised our research questions to be the following:

- What was the employee’s privacy knowledge of the accessibility and use of e-mail and office computers?
- What was the employee’s privacy knowledge concerning the personal use of email and office computers?
- What was the employee’s privacy knowledge regarding the administrative oversight of e-mail and office computers?

**Table 1: E-mail and Office Computer Factors and Items Within**

Item	Factor 1 Accessibility and Use (AU)	Factor 2 Personal Use (PU)	Factor 3 Administrative Oversight (AO)
Password creation and change procedures	.732		
Employees can be fired for misuse	.649		
Require an access code for e-mail	.642		
Policy about who can use the e-mail system	.639		
Computerized personnel files are secured*			
Use work computer for personal activities		.836	
Personal information is on office computer		.781	
Permission to use computer and e-mail for personal matters		.687	
Explanation of who has access to files kept on office computer			.772
Awareness of safeguards for copying and forwarding messages			.705
Other than myself, access to my business e-mail messages			.519

\*Discarded

**Table 2: Inter-Item Reliability (Cronbach's Alpha)**

Variable	Alpha
Accessibility and use	.6105
Personal use	.6728
Administrative oversight	.4327

## RESULTS

The demographic distributions of the responding sample are presented in Table 3. Because of the flexible quota, younger workers and those of higher educational and socioeconomic status are somewhat more represented in comparison to the public at large. The means and standard deviations for the accessibility and use (AU), personal use (PU) and administrative oversight (AO) variables are presented in Table 4.

### *THE ACCESSIBILITY AND USE OF E-MAIL AND OFFICE COMPUTERS*

We used *t* tests to compare the genders and length of time at position, more than or less than

one year. We found no significant differences for the privacy knowledge of accessibility and use of e-mail and office computers between the genders and the length of time at the position.

Analysis of variance was used to compare the response differences in accessibility and use of e-mail and office computers for the multiple category demographic characteristics family income level, age, highest level of education, and type of employment. We found no significant differences in privacy knowledge of the accessibility and use of e-mail and office computers for the different age categories. The mean AU score for all age categories fell between 3.58 and 3.75, signifying that people of all ages are aware that their organizations have password creation and change procedures, require access codes for e-mail, have policies about e-mail use, and can terminate the employment of those employees who misuse e-mail.

In the levels of education we found significant differences in the main effect,  $F(6, 1027) = 3.611, p = .002$ . Post hoc tests revealed differences in the responses between each of the three lowest education levels with two of the higher education levels. The Bachelor's category

**Table 3: Demographic Distributions of Responding Sample**

Characteristic	Number	%	Characteristic	Number	%
<i>Age</i>			<i>Family Income Level</i>		
22-29	234	22.3	Under \$25,000	92	8.8
30-39	206	19.7	\$25,000-49,999	231	22.0
40-49	221	21.1	\$50,000-74,999	249	23.8
50-59	223	21.3	\$75,000-99,999	187	17.8
60-69	164	15.6	Over \$100,000	275	26.2
<i>Sex</i>			<i>Length of Time at Position</i>		
Male	522	49.8	Less than one year	193	18.4
Female	526	50.2	A year or more	773	73.8
<i>Highest Level of Education</i>			<i>Type of Employment</i>		
Some high school	30	2.9	Government	120	11.5
High school graduate	135	12.9	Education	168	16.0
Some college	207	19.8	Self-employment	97	9.3
Associate degree	80	7.6	Company	434	41.4
Bachelor's	319	30.4	Homemaker	24	2.3
Master's	191	18.2	Retired	76	7.3
Beyond masters	83	7.9	Seeking employment	7	0.7
			Student	42	4.0
			Other	77	7.3

**Table 4: Means and Standard Deviations for Accessibility and Use (AU), Personal Use (PU), and Administrative Oversight (AO)**

Characteristic	AU Mean (SD)	PU Mean (SD)	AO Mean (SD)
<b>Sex</b>			
Female	3.66 (.871)	3.01 (1.035)	3.25 (.870)
Male	3.69 (.856)	3.21 (.999)	3.20 (.904)
<b>Length of Time at Position</b>			
Less than one year	3.51 (.908)	3.07 (.964)	3.19 (.918)
A year or more	3.72 (.857)	3.14 (1.038)	3.24 (.887)
<b>Age</b>			
22-29	3.65 (.868)	3.33 (.962)	3.15 (.863)
30-39	3.66 (.885)	3.20 (.979)	3.23 (.861)
40-49	3.75 (.852)	3.12 (1.059)	3.25 (.872)
50-59	3.72 (.847)	3.01 (1.043)	3.22 (.891)
60-69	3.58 (.867)	2.81 (1.006)	3.28 (.974)
<b>Education</b>			
Some high school	3.37 (.768)	2.90 (1.040)	3.27 (.764)
High school graduate	3.57 (.829)	2.65 (1.100)	3.33 (.794)
Some college	3.54 (.892)	3.06 (1.053)	3.15 (.895)
Associate degree	3.63 (.948)	2.94 (1.050)	3.30 (.962)
Bachelor's	3.78 (.861)	3.21 (.969)	3.22 (.871)
Master's	3.82 (.812)	3.42 (.921)	3.25 (.918)
Beyond masters	3.61 (.828)	3.14 (.877)	3.08 (.954)
<b>Family Income Level</b>			
Under \$25,000	3.67 (.812)	2.77 (1.085)	3.29 (.950)
\$25,000-49,999	3.64 (.849)	2.95 (1.046)	3.21 (.752)
\$50,000-74,999	3.49 (.879)	2.94 (1.032)	3.15 (.880)
\$75,000-99,999	3.69 (.849)	3.28 (.905)	3.19 (.957)
Over \$100,000	3.89 (.837)	3.39 (.968)	3.29 (.932)
<b>Type of Employment</b>			
Government	3.86 (.897)	3.07 (1.162)	3.37 (.878)
Education	3.68 (.784)	3.20 (.876)	3.11 (.953)
Self-employment	3.37 (.810)	3.52 (1.029)	3.43 (.920)
Company	3.83 (.835)	3.12 (1.043)	3.17 (.884)
Homemaker	2.98 (.815)	3.21 (.756)	3.23 (.743)
Retired	3.34 (.853)	2.81 (.839)	3.14 (.811)
Seeking employment	3.43 (.313)	3.33 (.860)	3.14 (.741)
Student	3.26 (.839)	3.09 (.929)	3.11 (.673)
Other	3.67 (.924)	2.72 (1.050)	3.43 (.885)

was significantly higher than Some High School ( $p = .014$ ), High School Graduate ( $p = .018$ ), and Some College ( $p = .002$ ). The Master's category was also significantly higher than Some High School ( $p = .009$ ), High School Graduate ( $p = .012$ ), and Some College ( $p = .001$ ). Two education categories, Associate Degree and Beyond Master's, did not have significant differences from other education categories.

The responses to those questions dealing with the accessibility and use of e-mail and office computers were found to be significant,  $F(4, 1018) = 7.331, p = .000$  across income levels. Post hoc tests showed that individuals with a

family income between \$50,000 and \$75,000 had significantly lower awareness than the highest income category ( $p = .000$ ). Individuals with family income over \$100,000 reported an elevated understanding of these accessibility issues.

Differences were also found when comparing accessibility and use for the eight employment categories ( $F(8, 1025) = 8.834, p = .000$ ). Privacy knowledge of the accessibility and use of e-mail and office computers by those employed by government, education, or commercial organizations varied significantly when compared to those who were self-employed, currently

homemakers, retired, seeking employment, or students. All post hoc tests for each of these comparisons exceeded the .01 significance level. This was an expected finding, considering that such organizations have password creation and change procedures, require access codes for e-mail, and have policies about e-mail abuse.

In general, we found that employees with higher incomes, higher levels of education, and those employed within larger and more formal organizations confirmed their awareness and knowledge of the fact that organizations have password creation and change procedures, require access codes for e-mail, and have policies about e-mail use. Respondents also acknowledged an understanding that employees who misuse e-mail can have their employment terminated. More than 35% of all employees, however, mostly those with lesser income and a lower level of education were not aware of e-mail and office computer privacy accessibility issues.

#### *PERSONAL USE OF E-MAIL AND OFFICE COMPUTERS*

We used *t* tests to determine the response differences between genders and between respondents with shorter or longer lengths of time in their positions. We found no significant differences in privacy knowledge of the personal use of e-mail and office computers between those with more than or less than one year in their positions. We did find a significant difference between males and females,  $t(1039) = -3.249$ ,  $p = .001$ .

Analysis of variance was used to determine the response differences in the personal use of e-mail and office computers for all multiple category demographic characteristics, age, family income level, highest level of education, and type of employment. We found significant differences for age,  $F(4, 1036) = 7.167$ ,  $p = .000$ . Post hoc tests showed that those 22 to 29 years of age reported a significantly higher personal use score than every other age category except those 30 to 39; all reached the .05 significance level. Post hoc tests also showed that those in the 30 to 39 ( $p = .000$ ) and 40 to 49 age levels ( $p = .004$ ) reported a significantly higher personal use score

than those 60 to 69. The overall trend revealed that the younger an employee is, the more he or she reported using a work computer for personal activities and storing personal information.

The level of education was also significant for personal use,  $F(6, 1031) = 9.023$ ,  $p = .000$ . Post hoc analysis showed that high school graduates reported less personal use than all other education levels, though all differences reached the .05 significance level. Also, those with bachelor's and master's degrees reported much higher personal use than all other education categories except Beyond Master's; all differences reached the .000 significance level. This demonstrates that more highly educated workers are more likely to use office computers for personal activities.

Family income was significant,  $F(4, 1022) = 12.523$ ,  $p = .000$ , for personal use. Post hoc analysis showed that the three lowest family income levels, those making \$74,999 and below, were significantly lower on the personal use measure than the two highest family income levels, \$75,000 and above; all reached the .05 significance level. Higher income earners were much more likely to report using an office computer for personal use.

The significant differences for the type of employment centered principally on those self-employed,  $F(8, 1029) = 4.499$ ,  $p = .000$ . The self-employed reported using a work computer for personal use significantly more than all of the employment categories except for those currently homemakers or seeking employment. All post hoc tests comparing the self-employed with students, the retired, and those working in government, education, or for a company reached the .05 significance level. This was expected because the self-employed may not differentiate between personal and work related activities.

#### *ADMINISTRATIVE OVERSIGHT OF ORGANIZATIONAL E-MAIL AND OFFICE COMPUTERS*

Using *t* tests, we found no significant differences in privacy knowledge of the administrative oversight for organizational e-mail and office computers between the genders or by the length

of time at the position. Analysis of variance revealed no significant difference for privacy knowledge of the administrative oversight for organizational e-mail and office computers in the different age categories, income levels, or education levels.

Knowledge of administrative oversight was significantly different by employment category,  $F(8, 1024) = 2.32, p = .018$ . Of those currently working and not self-employed, government employees were more likely to report that they are provided an explanation of who has access to files kept on their office computer, are aware of e-mail safeguards, and that others have access to office e-mail messages. Those in education and industry were less likely to be aware of these issues; all post hoc tests reached the .05 significance level.

Those self-employed reported the highest level of administrative oversight awareness. This was expected because the individual responding to the survey was usually the person overseeing the available e-mail and office computer technology.

## DISCUSSION AND CONCLUSIONS

### *THE ACCESSIBILITY AND USE OF E-MAIL AND OFFICE COMPUTERS*

In general, we found that those with higher incomes, higher levels of education, and those employed with larger and more formal organizations were more likely to report awareness and knowledge of their organizations' password creation and change procedures, requirements for e-mail access codes, policies about e-mail use, and their employers' ability to terminate those who misuse e-mail.

More than one third of employees surveyed were not aware of e-mail concerns regarding user names and password protections, and why these concerns are important to the organization. As reported by Duane and Finnegan (2004), e-mail policies are often vague, contradictory in practice, and poorly communicated. Consequently, employers need to provide education and information on e-mail and office computer

security concerns, especially for those workers that are less educated and lower paid.

One of the cornerstones of privacy regulation in the United States is the idea of notice. This component has led to formal privacy notice requirements in many laws. Consequently, a privacy policy is even more important today due to expanding international regulation and the increased reliance upon the use of privacy policies as a measuring stick for enforcement action (Nahra, 2007).

Businesses and organizations today are increasingly more dependent on e-mail and office technology. Employers make e-mail available to more and more employees, not as a convenience, but as a necessity in conducting business. As a result, employers have changed usage policies and altered the corporate culture's expectation of privacy in order to maintain a secure work environment.

### *PERSONAL USE OF E-MAIL AND OFFICE COMPUTERS*

Men most often reported they used a work computer for personal activities and stored personal information on an office computer. These findings agree with the general theory that men are more inclined to take risks, such as storing and using office computer equipment for personal use, even when they are aware certain actions are not permitted (Schubert, Brown, Gysler, & Brachinger, 1999).

Younger adults reported using office e-mail and computer technology most often for personal use, with an overall decreasing trend as respondents aged. It would be interesting to survey the population in 10 years to see if this trend continues. As society becomes increasingly wired, older workers may reflect the same values as their younger counterparts and use work-related information technologies interchangeably with personal technologies.

Our findings that higher educated and more affluent workers are more likely to use an office computer and e-mail for personal activities were surprising. Traditionally, employees with higher levels of education and incomes are more aware of work related policies. But these findings could

highlight the fact that well paid, educated workers move between an office computer and home computer seamlessly, unconcerned with the means of task completion and willing to do their work on any available computer.

Most employers allow a reasonable personal use of office e-mail and computers (Hoffman et al., 2003), and it appears that personal privacy issues are important to employees involved in education, industry, and governmental settings. Most employees of industrial, governmental, and educational organizations assume a more professional attitude concerning the personal use of e-mail and office computers. This contradicts results from Loch et al. (1998). They reported that attendees at an educational conference responded to monitoring of e-mail and office computer technology as an unethical privacy practice by the employer. Educators in our study recognized the ethical dilemma and responded similarly to those working in government and industry.

Employers are allowed to invade individual e-mail and office computer privacy for the better good of the organization. Thirty years ago, most Americans would balk at the idea of being denied basic privacy rights. Today, millions of Americans working in schools, offices, hospitals and factories have their office computer and personal use e-mail privacy disregarded in favor of organizational security. Privacy rights have been redefined (Stone, 2004).

#### *ADMINISTRATIVE OVERSIGHT OF ORGANIZATIONAL E-MAIL AND OFFICE COMPUTERS*

Government employees were more aware than others that someone, whether an information technology professional or supervisor, has access and oversight responsibilities for files stored in their computers. In addition, government employees were more aware of the safeguards for e-mail use, and that e-mail messages are not private communications. Those working in business and organizations did not report as high an awareness of these issues. Cappel (1995) reported similar results 10 years ago. During this time of increased computer and e-mail use, we

found it unusual that business organizations were not communicating oversight procedures more efficiently.

Business employees appear to be less adequately informed about administrative oversight of e-mail and office computer use, but still adhere to a higher level of personal privacy procedures while on the job. As reported by Duane and Finnegan (2004), there are gaps in how organizations monitor and control e-mail, and organizations are poor at updating and communicating e-mail and technology oversight policies. Government supervisors appear to be the only administrators that provide adequate information to employees concerning possible invasions of computer privacy.

The monitoring of employees in the workplace is not new. Courts consistently have allowed monitoring in the workplace and have held that surveillance of an employee's office computer and e-mail use does not violate the Constitution. Consequently, workers generally have no reasonable expectation of computer privacy if an employer makes its monitoring policy widely known.

#### *CONCLUSIONS*

Privacy issues concerning the accessibility, personal use, and administrative oversight of e-mail and office computers influence the work activities of employees daily. There are pockets of employees that are better informed concerning each privacy issue. Accessibility issues, such as password procedures and policies, are better understood by higher educated, upper income earners in larger and more formal organizations. Industry and government workers are better informed about e-mail and office computer personal use policies, and government employees are more aware of organizational safeguards and oversight responsibilities.

There is a definite need for universal awareness and understanding of accessibility, personal use, and administrative oversight issues involving e-mail and office computers. If organizations have e-mail and office computer privacy policies and procedures in place, these policies do not appear to be adequately

communicated to, or understood by, employees. Employers should emphasize the proper communication of these privacy policies and procedures. We recommend that a comprehensive approach and investment in ethical safeguards and computer privacy policies be undertaken in cooperation with human resources (Von der Embse, Desai, & Desai, 2004). In addition, training is strongly recommended to deepen employee understanding.

## REFERENCES

- Alderman, E. & Kennedy, C. (1995). *The right to privacy*. New York: Alfred A. Knopf.
- Alreck, P. L. & Settle R. B. (1995). *The survey research handbook: Guidelines and strategies for conducting a survey* (2<sup>nd</sup> ed.) New York: McGraw Hill.
- Cappel, J. J. (1995). A study of individuals' ethical beliefs and perceptions of electronic mail privacy. *Journal of Business Ethics*, 14(10), 819-827.
- Crane, A. (2005). Workplace privacy? Forget it!, Bankrate.com. Retrieved April 4, 2007, from <http://www.bankrate.com/brm/news/advice/20050718a1.asp>
- Crockcroft, S. (2002). Gaps between policy and practice in the protection of data privacy. *The Journal of Information Technology Theory and Application*, 4(3), 1-13.
- Duane, A. & Finnegan, P. (2004). Managing email usage: A cross case analysis of experiences with electronic monitoring and control. *Proceedings of the 6<sup>th</sup> International Conference on Electronic Commerce*, 229-238.
- Electronic Privacy Information Center. (2003). Workplace privacy. Retrieved December 12, 2005, from <http://www.epic.org/privacy/workplace/default.html>
- Egelko, B. (2006, August 8). Federal appeals court rules against workplace PC privacy. *The San Francisco Chronicle*.
- Flynn, N. & Majerus, S. (2003). New survey of workplace e-mail reveals disasters in the making: 66% of U.S. companies lack e-mail retention policy. *PR Newswire*, June 23.
- Fraser v. Nationwide Mutual Insurance Company*. 135 F. Supp. 2d 623, (E.D. Pa. 2001).
- Givens, B. (1997). *The privacy rights handbook: How to take control of your personal information*. New York: First Avon Books.
- Gramm-Leach-Bliley Act. (1999). Pub. L. No. 106-102, 113 Stat. 1338 (1999).
- Henderson, S. C., & Snyder, C. A. (1999). Personal information privacy: Implications for MIS managers. *Information and Management*, 36(4), 213-220.
- Hoffman, W. M., Hartman, L. P., & Rowe, M. (2003). You've got mail . . . and the boss knows it: A survey by the center of business ethics of companies' email and Internet monitoring. *Business and Society Review*, 108(3), 285-307.
- Kelleher, R. & Flynn, N. (2003). Workplace e-mail reveals disasters in the making, according to new survey by American Management Association, The ePolicy Institute and Clearswift. *Business Wire*, May 28.
- Kelly, E. P., McHenka, M. L., & Zielinski, S. (1999). A manager's guide to same-sex sexual harassment in the workplace. *Central Business Review*, 19(2), 14-21.
- Kovach, K. A., Jordan, J., Tansey, K., & Framinan, E. (2000). The balance between employee privacy and employer interests. *Business and Society Review*, 105(2), 289-298.
- Lane III, F. S. (2003). *The naked employee: How technology is compromising workplace privacy*. New York: American Management Association.
- Loch, K. D., Conger, S. & Oz, E. (1998). Ownership, privacy, and monitoring in the workplace: A debate on technology and ethics. *Journal of Business Ethics*, 17(6), 653-663.
- Muick v. Glenayre Electronics*, 280 F.3d 741 (7<sup>th</sup> Cir. 2002).
- Nahra, K. J. (2007). A privacy and security checklist: Focusing your attention on the most pressing issues. *Privacy and Security Law Report*, 6(2), 55-60.
- Privacy Rights Clearinghouse/UCAN. (2006, February). Fact sheet 7: Workplace Privacy. Retrieved April 2, 2007, from <http://www.Privacyrights.org/fs/fs7-work.htm>
- Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).
- Schubert, R., Brown, M., Gysler, M., & Brachinger, H. W. (1999). Gender and economic transactions—Financial decision-making: Are women really more risk-adverse? *The American Economic Review*, 89(2), 381-385.
- Smith, M. S. (2003, February 6). Internet privacy: Overview and pending legislation. Report for Congress. (CRS Report RL31408). Washington, DC: Congressional Research Service.

- Stone, A. (2004). The delicate balance: Security and privacy. *IEEE Security & Privacy Magazine*, 2(4), 12-13.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 146-169.
- Von der Embse, T. J., Desai, M. S., & Desai, S. (2004). How well are corporate ethics codes and policies applied in the trenches? *Information Management & Computer Security*, 12(2), 146-153.
- White, G. W., & Pearson, S. J. (2001). Controlling corporate e-mail, PC and computer security. *Information Management & Computer Security*, 9(2), 88-92.

#### Appendix. Survey Questions

- 1) My organization does not require an access code for e-mail.
- 2) My organization has a policy about who can use the e-mail system.
- 3) I use my work computer system for personal activities.
- 4) Employees are not permitted to use the computer and e-mail for personal matters.
- 5) An employee can be fired for misuse of computers or e-mail.
- 6) Someone other than me also has access to my business e-mail messages.
- 7) To maintain computer security, my employer has password creation and change procedures.
- 8) Computerized personnel files are strongly secured.
- 9) Employees are not provided an explanation of who has access to files kept in their office computer and under what circumstances.
- 10) Personal information is on my office computer.
- 11) In my job, I am not aware of safeguards for copying and forwarding messages.

Material published as part of this journal, either on-line or in print, is copyrighted by the Organizational Systems Research Association. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Donna Everett, [d.everett@moreheadstate.edu](mailto:d.everett@moreheadstate.edu) to request redistribution permission.