Available online at www.sciencedirect.com
ScienceDirect
Computers in Human Behavior 24 (2008) 1067–1084
Computers in Human Behavior
www.elsevier.com/locate/comphumbeh

Correlates of different forms of cyberloafing: The role of norms and external locus of control

Anita L. Blanchard [a,*], Christine A. Henle [b,1]

[a] University of North Carolina at Charlotte, Department of Psychology, Charlotte, NC 28223, United States
[b] University of North Carolina at Charlotte, Department of Management, Charlotte, NC 28223, United States

Available online 22 May 2007

Abstract

Cyberloafing is the personal use of email and the Internet while at work. The purpose of this study is to identify the different forms of cyberloafing and their antecedents. We propose that cyberloafing has two primary forms: minor cyberloafing (e.g., sending and receiving personal email at work) and serious cyberloafing (e.g., online gambling, surfing adult oriented web sites). Additionally, we hypothesize that employees' perceptions of coworker and supervisor norms supporting cyberloafing are related to minor cyberloafing but not serious cyberloafing. We also hypothesize that external locus of control (i.e., a belief that chance and powerful others determines one's outcomes), as an antecedent of other counterproductive work behaviors, will be related to both minor and serious cyberloafing. Two hundred and twenty two employed graduate business students were surveyed. Two forms of cyberloafing were identified: one composed of minor cyberloafing behaviors and one composed of the more serious cyberloafing behaviors. As predicted, employees' perceptions of their coworkers' and supervisor's norms were positively related to minor cyberloafing, but not related to serious cyberloafing. Also as predicted, belief in chance was positively related to both minor and serious cyberloafing. A belief in powerful others was not related to minor or serious cyberloafing. Implications for policy development to regulate cyberloafing in organizations are discussed.

Keywords: Computer mediated communication; Internet; Organizations; Antisocial behavior; Social norms

* Corresponding author. Tel.: +1 704 687 4847; fax: +1 704 687 3096.
E-mail addresses: alblanch@email.uncc.edu (A.L. Blanchard), cahenle@email.uncc.edu (C.A. Henle).
[1] Tel.: +1 704 687 3199; fax: +1 704 687 3123.

0747-5632/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chb.2007.03.008

1. Introduction

Cyberloafing (also called cyberslacking) is employees' non-work related use of company provided email and the Internet while working (Lim, 2002). Some of this cyberloafing can be considered rather innocuous, especially if limited in duration (e.g., sending and receiving a personal email or checking headlines at CNN.com). Other types of cyberloafing, however, are considered more of a problem either because they are more time consuming and thus reduce productivity (e.g., online shopping), they are inappropriate behavior at work (e.g., online gambling), or because they are expose organizations to legal liabilities (e.g., downloading music).

As access to the Internet has become more common for employees, so has their propensity to use the Internet for entertainment and other non-work purposes on the job. In 2000, 56% of employees were using the Internet for personal reasons (Greengard, 2002). By 2003, 59% of Internet use at work was non-work related (Griffiths, 2003). And by 2005, cyberloafing had become the most common way that employees waste time at work (Malachowski, 2005). Employees are also increasing the amount of time they spend cyberloafing. Current estimates range from a little over 3 h per week (Greenfield & Davis, 2002) to 2.5 h per day (Mills, Hu, Beldona, & Clay, 2001).

As cyberloafing increases, so do employers' concerns about it. Cyberloafing results in lost wages through decreased productivity (Malachowski, 2005; Scheuermann & Langford, 1997; Stewart, 2000). Further, employees' personal use of company technology can flood computing resources, which in turn clogs bandwidth and degrades system performance (Sipior & Ward, 2002). Cyberloafing can also put the organization at risk if the employee engages in illegal activities online (e.g., downloading music) or creates a harassing environment through viewing or sending offensive material (Lichtash, 2004; Mills et al., 2001; Panko & Beh, 2002; Scheuermann & Langford, 1997). Estimates are that between 20% and 30% of companies have fired an employee for cyberloafing including accessing pornographic sites, online gambling, and online shopping (AOM, 2003; Case & Young, 2002; Greenfield & Davis, 2002).

Although research on cyberloafing has been increasing, it has generally been descriptive (an exception is Lim, 2002) and often fails to differentiate among the types of cyberloafing, especially with regards to Internet use. We address this issue by arguing that there are different forms of cyberloafing and that these different forms have different antecedents. We feel that understanding the different forms of cyberloafing and their causes is important so that organizations can develop appropriate cyberloafing policies and sanctions. For example, policies may focus primarily on illegal activities (e.g., downloading music) which occur infrequently, but may not address more frequent forms of cyberloafing that are potentially more detrimental to employee productivity and computer resources (e.g., forwarding chain emails). Additionally, like other forms of inappropriate workplace behavior, there are likely to be different causes for the different forms of cyberloafing (see Robinson & Bennett, 1995). Policies and sanctions should therefore be appropriately designed.

1.1. Different types of cyberloafing

We believe that there is a tension in the literature that comes from combining all forms of cyberloafing into one type of work behavior. As indicated above, many researchers argue that cyberloafing is wasteful and opens the organization up for lawsuits. Other

researchers, however, do not believe that cyberloafing is necessarily bad or even inappropriate. They argue that the Internet provides a much needed diversion at work which can lead to creativity, flexibility, camaraderie, and foster a learning environment (Anandarajan, Devine, & Simmers, 2004; Anandarajan & Simmers, 2004; Belanger & Van Slyke, 2002; Block, 2001; Greenfield & Davis, 2002; Oravec, 2002; Stanton, 2002). Employees who engage in experimentation while cyberloafing may help develop important skills and knowledge which could make them more valuable to the organization (Anandarajan et al., 2004; Anandarajan & Simmers, 2004; Belanger & Van Slyke, 2002; Sunoo, 1996). These researchers argue that cyberloafing such as sending and receiving personal email is similar to taking personal phone calls at work and thus may be considered a perk. In summary, some researchers argue that cyberloafing may harm employers while others argue that it may enhance employee productivity.

We, therefore, propose that there are different types of cyberloafing. For example, checking one's personal email at work should be considered differently from surfing adult oriented sites at work. First, these different cyberloafing behaviors occur at different rates. Lim et al. (Lim, 2002; Lim & Teo, 2005; Lim, Teo, & Loo, 2002) found that viewing adult oriented sites was the least reported cyberloafing activity with only about 5% of the participants who reported engaging in this behavior on a regular basis whereas over 85% of the participants reported receiving non-work related emails at work. That is, the most delinquent forms of cyberloafing may be quite rare while the more innocuous forms may be much more common. This contention is supported in a study by Lim and Teo (2005) that found an inverse relationship between how frequently employees engaged in cyberloafing and how serious an offense they perceived it to be.

Anandarajan et al. (2004) report that employees and managers created distinct clusters of cyberloafing types including disruptive cyberloafing (e.g., adult web sites and online games), recreational cyberloafing (e.g., shopping and purposeless surfing) and personal learning cyberloafing (e.g., visiting professional groups and searching for news of the organization). However, these clusters were developed by respondents' perceptions about the appropriateness of the particular cyberloafing behavior at work and not by their actual behavior. Lim (2002) goes beyond perceptions and demonstrates that personal email use at work loads onto a separate behavioral factor from the Internet browsing activities she examined. Nevertheless, Lim's overarching cyberloafing typology is based on communication technology: email versus the Internet. We feel this is not the most appropriate typology, as we discuss below. For example, we argue that reading an Internet news site like CNN.com is more similar to checking one's personal email than online gambling or downloading music. Thus, we believe this typology ignores important differences among Internet activities.

We feel it is very important to identify and examine the different types of cyberloafing separately. First, it is important for organizations to understand what the different types of cyberloafing are and the frequency with which they occur. Second, by examining the different forms of cyberloafing separately, we are more likely to understand what leads to the different types of cyberloafing and also develop appropriate policies or interventions to decrease or manage their prevalence. For example, some researchers have argued that zero tolerance or overly aggressive cyberloafing policies may alienate employees, decrease job satisfaction or stifle creativity (Block, 2001; Greengard, 2002; Menzel, 1998). However, too lax policies can leave the organization open to lawsuits or simply decrease productivity at work (Mirchandani & Motwani, 2003; Siau, Nah, & Teng, 2002; Sipior & Ward, 2002). Organizations should tailor their policies to the different forms of cyberloafing.

Although we argue that there are different forms of cyberloafing, specifying which particular cyberloafing activities are related to which particular cyberloafing form is challenging. There has been neither sufficient nor consistent empirical research on the different forms of cyberloafing for us to propose which specific activities will fall under which forms. Additionally, the empirical research that has been conducted (e.g., Lim, 2002) occurred far enough in the past that new technologies (e.g., blogs, auction sites, instant messaging) have developed and become commonplace that were not included in previous research.

Nonetheless, we can anticipate general cyberloafing forms. Previous researchers (e.g., Lim, 2002) have referred to cyberloafing as a type of production deviance. That is, cyberloafing is a counterproductive behavior which detracts from an employee's level of performance at work. Robinson and Bennett (1995) developed a typology of deviant workplace behavior which provides insights into the cyberloafing forms we may anticipate. In their typology, they argue that deviant workplace behaviors can be divided into minor or serious on one dimension and interpersonally or organizationally focused on the other. As a form of production deviance, cyberloafing is an organizationally focused deviant behavior that can range from minor (e.g., checking one's personal email) to serious (e.g., downloading music illegally).

Following Robinson and Bennett's typology, we propose that there will be two main types of cyberloafing in which employees engage: minor and serious. We feel this provides a better way of conceptualizing cyberloafing (as opposed to legal/illegal or common/unusual) at work because of its grounding in deviance research. We anticipate that minor cyberloafing will consist of "common" uses of email and the Internet at work. For example, this form of cyberloafing may include sending and receiving personal email or visiting mainstream news, financial and sports related sites. In this way, minor cyberloafing is similar to other commonly tolerated although not entirely appropriate behaviors at work: taking personal phone calls, reading the Wall Street Journal at one's desk, and chatting by the water cooler. We must note that although we refer to this type of cyberloafing as minor, we do not mean to imply at all that it could not have detrimental effects on the organization such as reduced productivity. Instead, we argue that it is a qualitatively different form of deviance and, as we argue below, may have different antecedents.

We also anticipate that there will be another main form of cyberloafing consisting of more serious forms of cyberloafing, that is, those behaviors which researchers have previously warned are abusive and potentially illegal such as online gambling, downloading music, viewing adult oriented sites (Case & Young, 2002). Although we anticipate two main forms, this does not mean that we assume that there are only two facets of cyberloafing; we merely anticipate that there will be minor and serious form(s) of cyberloafing.

Therefore, we propose the following research question:

Research Question 1: What are the different forms of minor and serious cyberloafing?

1.2. Explanations of cyberloafing

Although identifying the types of cyberloafing in which employees engage in is important, it is only a first step. We also seek to understand the differences in why people engage in the different forms of cyberloafing. We believe that these differences are linked to an important conceptual distinction between employees who engage in minor cyberloafing and those who engage in the serious cyberloafing. That is, employees who engage in minor cyberloafing do not believe that they are engaging in inappropriate or deviant behavior

whereas employees who engage in serious cyberloafing realize it is deviant and not likely to be condoned at work.

Deviant behavior can be defined as behavior that departs from the norms of a reference group (Warren, 2003). Indeed, many of the researchers who discuss organizational policy related to cyberloafing imply that cyberloafing is a deviant work behavior because it violates company norms (cf., Mills et al., 2001; Mirchandani & Motwani, 2003; Siau et al., 2002). We argue that this approach is appropriate, but only for serious cyberloafing. Conversely, we propose that employees engaged in minor cyberloafing do not see it as deviant behavior at work. Instead, employees may see minor cyberloafing such as sending and receiving personal email as similar to making and taking personal phone calls at work, a behavior Robinson and Bennett (1995) describe as minor, organizationally focused deviant behavior. Taking personal phone calls at work is generally acceptable, although not always officially condoned, and usually falls within the norms of acceptable behavior.

Research on organizational socialization suggests that employees' norms of appropriate behavior come from their reference groups, primarily coworkers and supervisors (e.g., Ashford, 1986; Morrison, 1993). Thus, employees who engage in minor cyberloafing are doing so in response to perceptions that others in the organization also regularly use some forms of email and the Internet for personal use. Early research supports this approach. Lim and Teo (2005) report that employees justify their cyberloafing practices because "everybody else does it." Lee, Lee, and Kim (2004) show that social influence from coworkers and supervisors was related to frequency of and time spent cyberloafing. Anandarajan and Simmers (2004) even demonstrate that supervisors' norms vary on the appropriateness of cyberloafing. Some managers are cyber-bureaucrats who feel that employees should never engage in personal use of the web at work while others are cyber-humanists who believe personal use of the web can help balance employees' lives. Clearly, cyberloafing is related to norms and norms vary. However, none of this previous research has examined the relationship of norms with the different types of cyberloafing.

We argue that employees who engage in serious cyberloafing are *not* going to perceive that their behavior is within the norms of appropriate behavior at work. These forms of cyberloafing are more likely to be considered universally inappropriate at work (see Case & Young, 2002) and thus should not be related to employees' perceptions that others would engage in them or approve of them. Therefore, we hypothesize the following:

Hypothesis 1. Employee perceptions of coworker and supervisor norms supporting cyberloafing will be positively related to minor cyberloafing, but unrelated to serious cyberloafing.

We define serious cyberloafing as a deviant behavior because it is likely to go against the norms of the workgroup and supervisors. For example, in most organizations, coworkers and supervisors frown at a colleague who spends part of the workday gambling online or playing games. As such, we can turn to the counterproductive work behavior literature to understand why employees might engage in serious cyberloafing. In a recent analysis of the literature on the antecedents of counterproductive work behavior, Spector and Fox (2002) reported that locus of control, particularly, external locus of control, is a critical variable for understanding employees' voluntary behavior at work. Locus of control is defined as the extent to which individuals believe they have control over a situation (Rotter, 1966). People who have a high external locus of control believe that external events have more influence over a situation than they personally do.

Individuals who have a higher external locus of control are more likely to engage in counterproductive work behavior (Fox & Spector, 1999; Perlow & Latham, 1993; Spector & Fox, 2002). Fox and Spector (1999) additionally report that external locus of control is related to organizationally focused counterproductive work behavior, of which we argue serious cyberloafing would be an example. Spector and Fox (2002) also argue that as a generalized trait, external locus of control should be related to a wide variety of counterproductive work behaviors.

Although external locus of control can be considered as one construct, Levenson (1974) has effectively demonstrated that external locus of control has two important sub-facets: the belief in powerful others and the belief in chance. Additionally, the two facets may have different relationships to counterproductive behavior, and in this case, to serious cyberloafing. First, a belief in powerful others means that employees believe that others, particularly those higher up in the organization and with more authority, have a great deal of control over their destiny. We argue that employees with a strong belief in powerful others are likely to have a lower level of serious cyberloafing, because of the fear that they would be caught by these powerful others.

On the other hand, a higher belief in chance would be related to a higher level of serious cyberloafing. People who believe that chance plays a strong role in their lives believe that good and bad things happen to them for some unknown, external reason. This is essentially the direct opposite of an internal locus of control in which people believe good and bad things happen to them because of their personal actions. We, therefore, argue that people with a strong belief in chance will engage in more serious cyberloafing because whether or not they get caught is due to some random event and not due to anything they or anyone else does.

It is reasonable, then, to anticipate that external locus of control may be related to serious cyberloafing. What is its relationship to minor cyberloafing? Although we argue that minor cyberloafing is not deviant because employees are able to justify it as behavior that their peers and supervisors also engage in, employees may also recognize that it is not completely condoned behavior by the organization. For example, an occasional personal phone call may be considered a perk of the job and a behavior within the norms of the workgroup, but engaging in personal conversations over a long period of time would be considered inappropriate. We argue that similar logic applies to minor cyberloafing.

Thus, we hypothesize that external locus of control will be related to both serious and minor cyberloafing in the following ways:

Hypothesis 2a. Employees' belief in powerful others will be negatively related to serious and minor cyberloafing.

Hypothesis 2b. Employees' belief in chance will be positively related to serious and minor cyberloafing.

2. Method

2.1. Procedures and sample

Participants consisted of 221 employed MBA students at a Southeastern university. Although MBA students may be more driven than other employees, they allow researchers

to access employees at a range of levels across a variety of organizations. To be eligible for the study, participants had to be employed at least part time and have access to the Internet at work. Twenty surveys were omitted because participants did not meet the eligibility criteria, which resulted in a final sample of 201. Participants completed a survey regarding their demographics, perceptions of coworker and supervisor norms, external locus of control, and the frequency with which they engaged in cyberloafing. Participation was voluntary, but as an incentive those completing the survey were given a raffle ticket for a drawing of a $25 gift certificate to a local restaurant. A drawing was held during each class and took place immediately following completion of the survey so that no identifying information had to be collected, thus ensuring participants' anonymity.

Fifty-eight percent of the participants were male ($N = 117$) and the average age was between 36 and 45 years. The majority of participants were white (79%), followed by African American (7%), other (6%), Asian American (6%), and Latino (2%). Most participants worked for companies with over 500 employees (63%). Participants held a variety of jobs including supervisory (37%), financial (19%), accounting (14%), engineering (11%), information technology (6%), sales (3%), and education (2%).

2.2. Measures

2.2.1. Norms

Norms were measured by four items assessing the participants' beliefs that their coworkers and supervisors would approve of them using email and the Internet for personal use (e.g., "My coworkers would approve of me using the Internet for non-work related purposes" and "My coworkers would approve of me receiving/sending non-work related email"). The referent "coworker" was changed to "supervisor" to assess supervisor norms. A 5-point scale was used to measure participants' agreement with each item (1 = strongly disapprove to 5 = strongly approve).

2.2.2. External locus of control

External locus of control was measured using a scale developed by Levenson (1974). This scale measures two facets of external locus of control: chance and powerful others. The chance scale has eight items that assess the belief that events occur due to chance or fate (e.g., "When I get what I want, it's usually because I'm lucky." and "To a great extent my life is controlled by accidental happenings."). The belief in powerful others was measured using eight items that reflect the belief that consequences in life are determined by powerful other people (e.g., "Getting what I want requires pleasing those people above me." and "My life is chiefly controlled by powerful others."). Both the chance and powerful others measures used a 7-point response scale ranging from 1 = strongly disagree to 7 = strongly agree and had coefficient alphas of .77 and .78, respectively.

2.2.3. Cyberloafing

The cyberloafing measure contained 22 items. Eight of the items are from Lim's (2002) cyberloafing scale while the others were generated by the authors after reviewing the literature on cyberloafing. Respondents used a 5-point scale to specify the frequency over the past month that they engaged in cyberloafing ranging from 1 = never to 5 = a great deal. The items for this scale can be found in Appendix A.

2.2.4. Control variables

The following demographics were controlled for to ensure that the relationships between the antecedents and cyberloafing are not confounded: gender (0 = male, 1 = female), age (1 = 18–25 years, 2 = 26–35 years, 3 = 36–45 years, 4 = 46–55 years, 5 = 56–65 years, 6 = over 65 years), Internet skill (1 = beginner, 2 = intermediate, 3 = advanced, 4 = expert), and percent of time Internet is needed to do participant's job.

3. Results

Our first step in understanding cyberloafing at work was to examine the frequency with which respondents engaged in the different cyberloafing behaviors. Because of the number of cyberloafing behaviors we examined, we divided them into two figures. Fig. 1 presents the cyberloafing behaviors that approximately 50% of the participants reported that they had engaged in to some degree. For example, approximately 96% of our participants reported that they had received non-work related email while at work (conversely, only 4% have never received personal email at work) and approximately 46% have engaged in job hunting while at work. Fig. 2 reports the least frequent cyberloafing behaviors. For example, just under 40% of the participants reported ever participating in an online auction at work while just under 10% reported ever visiting adult web sites while at work.

We conducted an exploratory factor analysis with the cyberloafing and norms items in order to identify the different forms of cyberloafing (Research Question 1) and to check the validity of the norms items that we created for this study. We used a principal factors extraction because the items were non-normally distributed (see Fabrigar, Wegener, MacCallum, & Straham, 1999) and allowed the factors to correlate by using promax rotation.

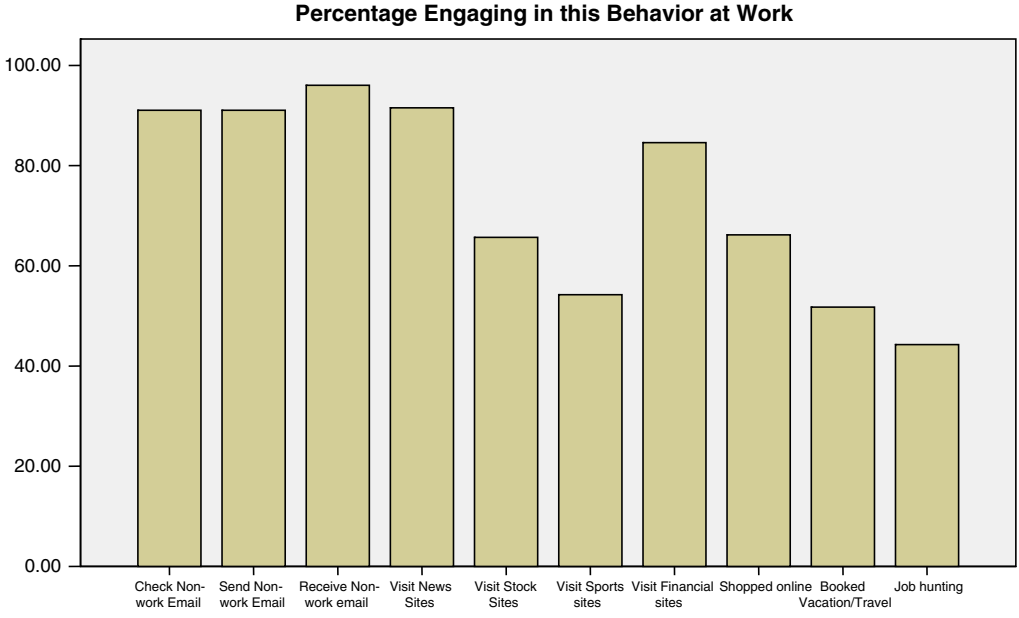

Fig. 1. Most common cyberloafing behaviors.

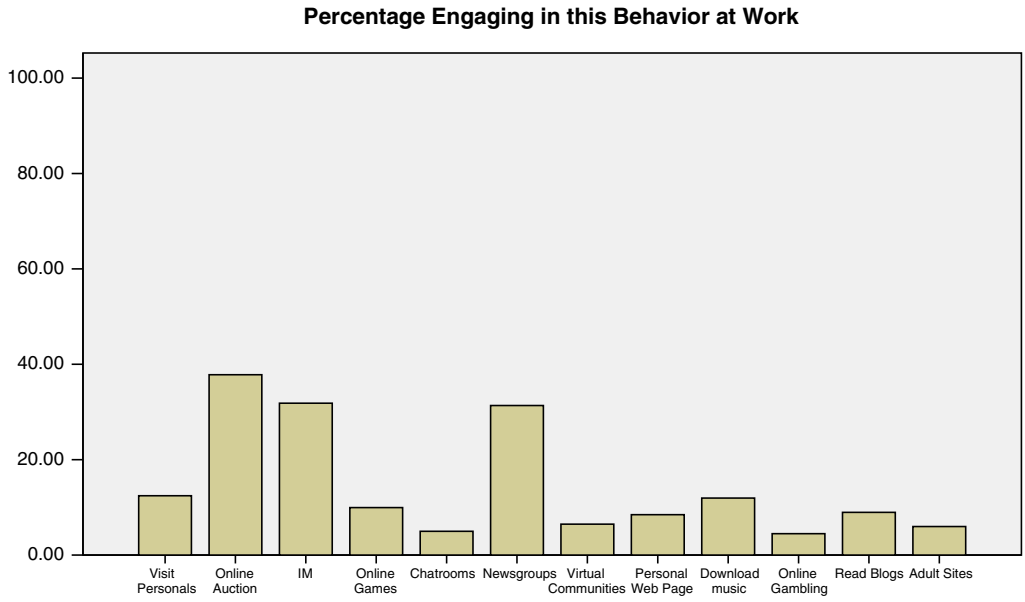

Fig. 2. Least common cyberloafing behavior.

Recently, research methodologists have strongly argued that factors in all factor analyses should be allowed to correlate instead of assuming the factors are orthogonal (Costello & Osborne, 2005; Fabrigar et al., 1999). The benefit of allowing the factors to correlate is that if the resulting component correlation matrix reports a low correlation, then the factors can be considered orthogonal. Otherwise, the analysis already takes into consideration a relationship between the resulting factors.

The KMO of .80 indicates the data are appropriate for factor analysis. An examination of the diagonals of the anti-image correlation matrix indicates that there is not a problem with multi-colinearity (Hutcheson & Sofroniou, 1999). The scree plot indicates that five factors should be selected, but this method of choosing factors can be too conservative and researchers are often advised to extract one or more factors than those suggested by the scree plot (Gorsuch, 1983). Because over-factoring (selecting too many factors) is preferable to under-factoring (choosing too few variables; see Fabrigar et al., 1999), we initially extracted six factors to see if there was adequate fit. However, the sixth factor only loaded one item. Recommendations are that factors must have three or more items loading over .50 to be included in the factor analysis (Costello & Osborne, 2005; Fabrigar et al., 1999). We then examined the five, four, and three factor solutions and determined that the three factor solution had both adequate items loaded (i.e., greater than four) as well as adequate strength of loading (i.e., all items had a factor loading greater than .50).

After the three factor solution was created, we examined the communalities and the item loadings. Communalities report the percent of the variance in a given variable explained by all the factors and is, in a sense, a measure of reliability of the variable (Gorsuch, 1983). A low communality suggests that the variable does not fit well in the factor structure. Four items had low communalities (i.e., less than .30) and did not logically fit with the factors onto which they loaded. These items were sequentially eliminated from

subsequent analyses. These items were instant messaging, booking vacation or travel, newsgroups, and online games. The remaining items and the factors onto which they loaded are in Table 1.

Component 1 consists of checking, receiving and sending personal email at work as well as surfing mainstream web sites including news, financial, auction, stock and sports sites and shopping online. We therefore consider this to be the "typical" cyberloafing at work and call the factor *minor cyberloafing*.

Components 2 consists of what we consider serious cyberloafing at work with the strongest item loading as surfing adult oriented sites. The remaining items include visiting chatrooms, virtual communities, personals and gambling sites, updating one's webpage, reading blogs and downloading music. Serious cyberloafing can be considered orthogonal to minor cyberloafing given their relatively low correlation ($r = .27$). The validity of these measures as minor and serious cyberloafing is strengthened because the items load in a conceptually coherent pattern and the factors are orthogonal.

Component 3 consists of the items we created for this study to assess coworker and supervisor norms, which supports their conceptual validity. This component is correlated to minor cyberloafing ($r = .49$) but is not correlated to serious cyberloafing ($r = .11$), which is to be expected based on our hypotheses. Because the items load separately and onto the factors we expected, this factor analysis supports that common method bias is not a major concern in our analysis (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003).

Table 1
Factor analysis of cyberloafing items and norms items (pattern matrix)

	Component		
	1	2	3
Receive non-work email	.89		
Send non-work email	.86		
Visit news sites	.77		
Check non-work email	.76		
Visit financial sites	.64		
Visit stock sites	.55		
Shop online	.59		
Visit sports sites	.47		
Online auctions	.40		
Visit adult oriented sites		.82	
Participate in chat rooms		.74	
Maintain personal web page		.61	
Visit virtual communities		.59	
Visit gambling sites		.58	
Check personals		.54	
Read blogs		.45	
Download music		.52	
Supervisor Internet norm			.88
Supervisor email norm			.88
Coworker Internet norm			.82
Coworker email norm			.82
Eigenvalue	6.60	3.26	2.02
% of Variance	30.14	14.82	9.17

We then combined the items from each cyberloafing component into two separate scales to use in the analyses. Table 2 presents the descriptive analyses of these scales and the study variables. Participants reported engaging in minor cyberloafing sometimes ($M = 2.74$, $SD = .83$) and engaging in serious cyberloafing only rarely ($M = 1.14$, $SD = .32$). In addition, gender was negatively correlated ($r = -.16$; $p < .05$) while Internet skill ($r = .19$; $p < .01$) and norms ($r = .43$; $p < .001$) were positively related to minor cyberloafing. Belief in powerful others ($r = .14$; $p < .05$) and chance ($r = .21$; $p < .01$) were the only significant correlates of serious cyberloafing. Thus, males, those with greater Internet skill, or individuals who perceive norms supporting cyberloafing were more likely to engage in minor cyberloafing while those who perceive powerful others or chance as controlling their destiny were more likely to participate in serious cyberloafing.

We then used the following strategy to test our hypotheses. First, we predicted that norms would be related to minor cyberloafing but not to serious cyberloafing. Second, we predicted that external locus of control would be related to both minor and serious cyberloafing. To simplify the analyses, we conducted two hierarchical regressions: one for minor and one for serious cyberloafing. In the first step we entered the control variables. In the second step, we entered in the norms measure. In the third step, we entered the locus of control variables. This strategy allows us not only to test the contribution of the individual variables (i.e., norms, powerful others and chance), but also allows us to test the contribution of the family of variables (i.e., locus of control). The results of the analyses do not change whether we enter external locus of control or norms first. Tables 3 and 4 present the results of these analyses.

Table 3 reports the analyses for minor cyberloafing. The control variables in Step 1 explain 6% of the variance minor cyberloafing with Internet skill ($\beta = .15$, $p < .05$) being the primary driver. In Step 2, the norms variable ($\beta = .41$, $p < .001$) contributes an additional 16% of the variance. That is, the more the employees believe their coworkers and supervisors approve of their use of the Internet and email for personal purposes, the more likely they are to engage in minor cyberloafing. Finally, belief in chance ($\beta = .19$, $p < .05$) had a moderately strong relationship to minor cyberloafing as predicted. This indicates that as employees have a stronger orientation towards the role of chance in determining their fate, they are more likely to engage in minor cyberloafing. The external locus of control variables as a group, however, only explained an additional 2% of variance beyond the control and norms measures.

Table 2
Descriptive analyses of study variables

Name	Mean	SD	1	2	3	4	5	6	7	8	9
1. Minor cyberloafing	2.74	.83	(.86)								
2. Serious cyberloafing	1.14	.32	.30***	(.80)							
3. Gender	1.37	.46	−.16*	−.05	(–)						
4. Age	2.01	.67	−.05	.02	−.15*	(–)					
5. Time on Internet	2.01	.68	.12	.06	−.02	−.13	(–)				
6. Internet skill	25.63	25.65	.19**	.12	−.30***	−.11	.12	(–)			
7. Norms	3.34	.85	.43***	.14	.02	−.02	.06	.17**	(.91)		
8. Powerful others	3.62	.77	−.02	.14*	.03	−.05	−.15*	−.08	.02	(.78)	
9. Chance	3.21	.85	.09	.21**	−.01	−.10	−.15*	−.13	−.02	.61***	(.78)

Note: $N = 201$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$. Reliabilities are in parentheses along the diagonal. (–) Indicates the measure is one item and does not have a reliability coefficient.

Table 3
Hierarchical regression for minor cyberloafing

	ΔR^2	B	SE of B	β
Step 1	.06*			
Gender		−.20	.13	−.12
Age		−.04	.09	−.04
Time on Internet		.00	.00	.09
Internet skill		.18	.08	.15*
Step 2	.16***			
Gender		−.24	.12	−.14
Age		−.05	.08	−.04
Time on Internet		.00	.00	.08
Internet skill		.08	.08	.07
Norms		.40	.06	.41***
Step 3	.02*			
Gender		−.22	.11	−.13
Age		−.03	.08	−.02
Time on Internet		.00	.00	.09
Internet skill		.11	.08	.09
Norms		.40	.07	.41***
Power		−.11	.08	−.11
Chance		.18	.08	.19*

Note: Total adjusted $R^2 = .21$, $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

Table 4 reports the results for serious cyberloafing. Steps 1 and 2 demonstrate that neither the control nor the norms variables significantly predicted this form of cyberloafing. As predicted, the external locus of control variables explained 7% of the variance beyond the aforementioned variables with chance driving this effect ($\beta = .23$, $p < .01$). This indicates that as employees have a stronger belief that chance determines their fate, the more likely they are to engage in serious cyberloafing.

In conclusion, Hypotheses 1, employees' beliefs regarding their coworkers' and supervisor's norms would explain minor cyberloafing but not serious cyberloafing, is supported. Hypotheses 2a and 2b, external locus of control would explain both employees' minor and serious cyberloafing, are only partially supported. Chance is related to both minor and serious cyberloafing loafing, but a belief in powerful others is not.

4. Discussion

The purpose of this study was to determine the forms of cyberloafing in which employees engage in and their antecedents. We identified two forms of cyberloafing: (a) minor cyberloafing consisting of sending and receiving personal email at work as well as surfing mainstream news and financial web sites and shopping online and (b) serious cyberloafing consisting of visiting adult oriented web sites, maintaining one's own web site and interacting with others online through chatrooms, blogs, and personals ads, gambling online, and downloading music.

Previous research has tried to categorize cyberloafing by either grouping activities as email or Internet based (Lim et al., 2002) or through people's perceptions of cyberloafing (Anandarajan & Simmers, 2004). The current study creates cyberloafing categories using

Table 4
Hierarchical regression for serious cyberloafing

	ΔR^2	B	SE of B	β
Step 1	.02			
Gender		−.01	.05	−.01
Age		.02	.04	.04
Time on Internet		.00	.00	.04
Internet skill		.05	.04	.11
Step 2	.01			
Gender		−.01	.05	−.02
Age		.02	.04	.04
Time on Internet		.00	.00	.04
Internet skill		.04	.04	.09
Norms		.04	.03	.11
Step 3	.07**			
Gender		.00	.05	.00
Age		.04	.03	.07
Time on Internet		.00	.00	.08
Internet skill		.06	.04	.13
Norms		.04	.03	.10
Power		.02	.03	.04
Chance		.09	.03	.23**

Note: Total adjusted $R^2 = .06$, $^{**}p < .01$.

actual employee behavior and is grounded in a theoretically and empirically based typology of deviant work behavior (cf., Robinson & Bennett, 1995). Nonetheless, there are two challenges for creating a definitive typology of cyberloafing behaviors. First, communication and collaboration technologies develop quickly. Networking software such as MySpace.com and FaceBook have quickly become very popular and relatively mainstream socializing technologies. Second, attitudes about the appropriateness of the technologies at work change. For example, instant messaging and blogs were once considered completely inappropriate at work, but some organizations are now using these technologies as ways to connect and inform their employees (see Cameron & Webster, 2004; Stross, 2006).

Similarly to previous research (Lim & Teo, 2005), employees in our study reported engaging in the minor form of cyberloafing much more frequently than engaging in the serious form of cyberloafing. Employees reported engaging in minor cyberloafing sometimes and serious cyberloafing rarely. Nearly 90% the participants reported receiving, checking and sending email quite frequently as well as visiting news and financial web sites. Less than 10% of the participants reported ever visiting chatrooms, engaging in online gambling, or visiting virtual communities or adult oriented web sites. Thus, the minor forms of cyberloafing are more typical in organizations than the more serious forms. Additionally, the potential costs of these behaviors (e.g., lost productivity, legal liability) justify the research to reveal their antecedents.

As we expected, employees' perceptions of the norms of their reference groups were related to minor cyberloafing. This relationship was strong as it explained 16% of the variance in minor cyberloafing. This finding supports our argument that employees do not consider minor cyberloafing to necessarily be deviant or inappropriate behavior. Employ-

ees believe that others, including their coworkers and supervisors, are using email and the Internet for personal reasons, too. This finding implies that employers and managers who want to develop policies to decrease minor cyberloafing should focus on changing employees' perceptions that checking email and surfing mainstream web sites are appropriate behavior while at work. Conversely, organizations may want to consider acknowledging that this behavior occurs and focus on regulating it. Some researchers argue that personal email and Internet use at work can be appropriate if certain conditions are met. For example, if job performance is not affected, the privilege is not abused (e.g., Holtz, 2001), and it does not interfere with normal business activities (Welebir & Kleiner, 2005), then a small amount of minor cyberloafing could be acceptable.

Employees' perceptions of norms were not related to serious cyberloafing. When engaging in these types of cyberloafing activities, employees do not feel that their coworkers and supervisors would approve. Essentially, employees know these behaviors are inappropriate at work. This finding agrees with Ananarajan et al.'s (Anandarajan et al., 2004; Anandarajan & Simmers, 2004) research showing that coworkers and managers have negative attitudes about specific forms of cyberloafing, particularly the ones we refer to as serious. This finding implies that educating employees that this sort of behavior at work is wrong will not be effective. They are already aware that they are not engaging in sanctioned behavior at work.

As predicted, external locus of control was related to both minor and serious cyberloafing. However, only a belief in chance provided a unique contribution in explaining both types of cyberloafing. A belief in powerful others was not related to either minor or serious cyberloafing. These findings suggest that employees who engage in minor or serious cyberloafing do not think that more powerful people up the organizational hierarchy will catch their inappropriate behavior. If they did, they would be less likely to engage in cyberloafing. Instead, the results suggest that people who cyberloaf believe that getting caught is up to chance. That is, the consequences of their behavior are due to bad luck.

Both of these findings imply that simply publicizing organizational policies and sanctioning is not likely to affect these employees' cyberloafing behavior because they think getting caught is random. We suggest that organizations need to develop and advertise policies as well as implement enforcement mechanisms. For example, monitoring software could be used to track employees' email and Internet activity and determine any inappropriate use. This would remove employee perceptions that the likelihood of getting caught for unacceptable activity is random or due to chance. However, monitoring activities need to be followed up with disciplinary actions, especially for the serious cyberloafing, in order to reinforce the inappropriateness of these activities. When developing these policies, organizations need to consider how stringent they want to be. Zero tolerance policies may result in feelings of mistrust between management and employees while no regulations could expose organizations to legal liabilities. Organizations must decide how much cyberloafing they will allow as some forms, especially minor cyberloafing, may be effective in reducing stress, balancing work and family, generating ideas, networking, and so forth.

There is a great deal yet to be learned about employees who engage in cyberloafing. Although significant, a relatively small proportion of the variance in serious cyberloafing was explained. Future research should continue to pursue serious cyberloafing as a counterproductive work behavior and to examine other variables of interest in this area of research. Although Lim (2002) examined justice (often related to counterproductive work behavior) and cyberloafing, we recommend examining the roles of personality character-

istics (e.g., conscientiousness, openness to new experience, moral disengagement) as well as environmental factors (e.g., job design, organizational climate) in future research. Although the serious forms of cyberloafing are not common, they are frequent and potentially harmful enough to warrant further understanding why employees engage in this sort of behavior and how it can be discouraged.

4.1. Limitations

All research contains limitations. In this study, one limitation is that our measures of coworker and supervisor norms are self-report. We do not know whether the norms our participants report are what others in the workplace would also report. We try to make the distinction clear that what we have analyzed is the employees' perceptions of their workplace norms as opposed to an objective (or group level) measure of norms. However, Fishbein and Ajzen (1975) emphasize the significant influence perceived norms can have on behavioral intentions and subsequent behaviors. Specifically, these researchers assert that individuals' perceptions of what behaviors referent others think they should or should not engage in will affect their behavioral decisions. Indeed, much research supports the positive relationship between individuals' perceptions of the approval of particular behaviors by referent others and the subsequent occurrence of these behaviors (e.g., Albarracin, Johnson, Fishbein, & Muellerleile, 2001; Becker, Randall, & Riegel, 1995; Harrison, 1995).

Along the same lines, our measure of cyberloafing is also self-report. As a potentially undesirable work behavior, it is possible that participants underreported their cyberloafing behaviors. As a result, the tests of our hypotheses may be conservative and understate the true nature of these relationships. However, we took appropriate precautions to deal with this problem of social desirability. First, we kept all participants' identity anonymous. This is highly important in increasing participants' trust and their likelihood of being honest in their responses (see Podsakoff et al., 2003). We also surveyed participants away from their work environments which is more likely to result in honest responding.

Finally, our sample consisted of MBA students who were employed at least part time. These are likely to be ambitious men and women who may have a stronger internal locus of control than the average employee. Although our data show a range of scores in the measures of chance and powerful others, it is possible that this population is different from the typical employee. For instance, other employees may have more fear of powerful others than MBA students who are hoping to become one of them. Future research should pursue the relationship between cyberloafing and other populations to expand the universality of our finding.

In conclusion, cyberloafing is a multi-faceted behavior which is likely to continue in organizations for the foreseeable future. We can fully expect that technological applications will continue to develop (e.g., podcasts, video downloads, networking spaces) and become available in the workplace. It is likely that cyberloafing will become more prominent and not less. Thus, we need to better understand what sorts of cyberloafing behaviors employees engage in and how we can minimize the negative effects of cyberloafing on worker productivity while still maintaining a workplace that allows for creativity and trust.

Appendix A. Cyberloafing items

Checked non-work related email
Sent non-work related email
Visited general news sites
Visited stock or investment related web sites
Checked online personals
Viewed sports related web sites
Received non-work related email
Visited banking or financial related web sites
Shopped online for personal goods
Visited online auctions sites (e.g., Ebay)
Sent/received instant messaging
Participated in online games
Participated in chat rooms
Visited newsgroups or bulletin boards
Booked vacations/travel
Visited virtual communities
Maintained a personal web page
Downloaded music
Visited job hunting or employment related sites
Visited gambling web sites
Read blogs
Viewed adult oriented (sexually explicit) web sites

References

Albarracin, D., Johnson, B. T., Fishbein, M., & Muellerleile, P. A. (2001). Theories of reasoned action and planned behavior as models of condom use: A meta-analysis. *Psychological Bulletin, 127*, 142–161.

Anandarajan, M., Devine, P., & Simmers, C. (2004). A multidimensional scaling approach to personal web usage in the workplace. In M. Anandarajan & C. Simmers (Eds.), *Personal web usage in the workplace: A guide to effective human resource management*. Hershey, PA: Information Science Publishing.

Anandarajan, M., & Simmers, C. (2004). Constructive and destructive personal web use in the workplace: Mapping employee attitudes. In M. Anandarajan & C. Simmers (Eds.), *Personal web usage in the workplace: A guide to effective human resource management*. Hershey, PA: Information Science Publishing.

AOM (2003). *E-mail rules, policies and practices survey*. American Management Association.

Ashford, S. J. (1986). Feedback-seeking in individual adaptation: A resource perspective. *Academy of Management Journal, 29*, 465–487.

Becker, T. E., Randall, D. M., & Riegel, C. D. (1995). The multidimensional view of commitment and the theory of reasoned action: A comparative evaluation. *Journal of Management, 21*, 617–638.

Belanger, F., & Van Slyke, C. (2002). Abuse or learning? *Communications of the ACM, 45*, 64–65.

Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics, 33*, 225–231.

Cameron, A. F., & Webster, J. (2004). Unintended consequences of emerging communication technologies: Instant messaging in the workplace. *Computers in Human Behavior, 21*, 85–103.

Case, C. J., & Young, K. S. (2002). Employee Internet management: Current business practices and outcomes. *CyberPsychology and Behavior, 5*, 355–361.

Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most out of your data. *Practical Assessment, Research and Evaluation, 10*(7), 1–9.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Straham, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods, 3*, 272–299.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fox, S. A., & Spector, P. E. (1999). A model of work frustration-aggression. *Journal of Organizational Behavior, 20*, 915–931.

Gorsuch, R. L. (1983). *Factor analysis*. Hillsdale, NJ: Sage.

Greenfield, D. N., & Davis, R. A. (2002). Lost in cyberspace: The web @ work. *CyberPsychology and Behavior, 5*, 347–353.

Greengard, S. (2002). The high cost of cyberslacking. *Workforce, 12*(December), 22–24.

Griffiths, M. (2003). Internet abuse in the workplace: Issues and concerns for employers and employment counselors. *Journal of Employment Counseling, 40*, 87–96.

Harrison, D. A. (1995). Volunteer motivation and attendance decisions: Competitive theory testing in multiple samples from a homeless shelte. *Journal of Applied Psychology, 80*, 371–385.

Holtz, S. (2001). Employees online: The productivity issue. *Communication World, 18*(2), 17–23.

Hutcheson, G., & Sofroniou, N. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models*. Thousand Oaks, CA: Sage.

Lee, Z., Lee, Y., & Kim, Y. (2004). Personal web use in organizations. In M. Anandarajan & C. Simmers (Eds.), *Personal web usage in the workplace: A guide to effective human resource management*. Hershey, PA: Information Science Publishing.

Levenson, H. (1974). Activism and powerful others: Distinctions within the concept of internal–external control. *Journal of Personality Assessment, 38*(4), 377–383.

Lichtash, A. E. (2004). Inappropriate use of e-mail and the Internet in the workplace: The arbitration picture. *Dispute Resolution Journal, 59*(February/April), 26–36.

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior, 23*, 675–694.

Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information and Management, 42*, 1081–1093.

Lim, V. K. G., Teo, T. S. H., & Loo, G. L. (2002). How do I loaf here? Let me count the ways. *Communications of the ACM, 45*, 66–70.

Malachowski, D. (2005). Wasted time at work costing companies billions. Retrieved December 15, 2005, from http://www.salary.com/careers/layoutscripts/crel_display.asp?tab=cre&cat=nocat&ser=Ser374&part=Par555.

Menzel, D. C. (1998). www.ethics.gov: Issues and challenges facing public managers. *Public Administration Review, 58*, 445–452.

Mills, J. E., Hu, B., Beldona, S., & Clay, J. (2001). Cyberslacking! A liability issue for wired workplaces. *Cornell Hotel and Restaurant Administration Quarterly, 42*, 34–47.

Mirchandani, D., & Motwani, J. (2003). Reducing Internet abuse in the workplace. *SAM Advanced Management Journal, 68*, 22–55.

Morrison, E. W. (1993). Longitudinal study of the effects of information seeking on newcomer socialization. *Journal of Applied Psychology, 78*, 173–183.

Oravec, J. A. (2002). Constructive approaches to Internet recreation in the workplace. *Communications of the ACM, 45*, 60–63.

Panko, R. R., & Beh, H. G. (2002). Monitoring for pornography and sexual harassment. *Communications of the ACM, 45*, 84–87.

Perlow, R., & Latham, L. L. (1993). Relationship of client abuse with locus of control and gender: A longitudinal study. *Journal of Applied Psychology, 78*, 831–844.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*, 879–903.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behavior: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555–572.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monograph, 80*(1), Whole No. 609.

Scheuermann, L. S., & Langford, H. P. (1997). Perceptions of Internet abuse, liability, and fair use. *Perceptual and Motor Skills, 85*, 847–850.

Siau, K., Nah, F. F., & Teng, L. (2002). Acceptable Internet use policy. *Communications of the ACM, 45*, 75–79.

Sipior, J. C., & Ward, B. T. (2002). A strategic response to the broad spectrum of Internet abuse. *Information Systems Management, 19*, 71–79.

Spector, P. E., & Fox, S. A. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource Management Review, 12*, 269–272.

Stanton, J. M. (2002). Company profile of the frequent Internet user. *Communications of the ACM, 45*, 55–59.

Stewart, E. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Security Management, 9*, 46–52.

Stross, R. (2006). All the Internet's a stage. Why don't C.E.O.'s use it? *The New York Times*, July 20.

Sunoo, B. P. (1996). This employee may be loafing. *Personnel Journal, 75*, 54–61.

Warren, D. E. (2003). Constructive and destructive deviance in organizations. *Academy of Management Review, 28*(4), 622–632.

Welebir, B., & Kleiner, B. (2005). How to write an acceptable Internet usage policy. *Journal of Management Research News, 28*, 80–87.