Computers in Human Behavior 29 (2013) 812–820

Contents lists available at SciVerse ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

The effects of sanctions and stigmas on cyberloafing

Joseph C. Ugrin [a,*], J. Michael Pearson [b,1]

[a] Department of Accounting, Kansas State University, Manhattan, KS 66502, USA
[b] Department of Management, Southern Illinois University, Carbondale, IL 62901, USA

ARTICLE INFO

Article history:
Available online 16 January 2013

Keywords:
Cyberloafing
Sanctions
Detection
Enforcement
Abusiveness
Deviance

ABSTRACT

Cyberloafing has become a pervasive problem for many organizations and some researchers have suggested that a deterrence approach utilizing acceptable use policies for Internet-based applications coupled with mechanisms designed to monitor employee Internet usage and detect unauthorized usage can be an effective way to reduce it. However, the results of studies that have examined the effects of acceptable use policies and detection mechanisms on reducing cyberloafing are mixed. This study attempts to reconcile those inconsistencies by using an experiment to show that the deterrence model affects various types of cyberloafing differently. The results reveal that individually, threats termination and detection mechanisms are effective deterrents against activities like viewing pornography, managing personal finances, and personal shopping, but must be coupled together and actively enforced to dissuade activities like personal emailing and social networking.

1. Introduction

Internet resources are important components of the workplace and are being used to improve work performance in a number of ways (Whitty & Carr, 2006). Yet they can also be abused – particularly by employees using these resources excessively for personal purposes (cyberloafing).[2] Employees cyberloaf by participating in activities like online shopping, personal investment management, social networking, emailing, and viewing online media (Blanchard & Henle, 2008; Lim, Teo, & Loo, 2002; Ugrin & Pearson, 2008) and do so for a number of reasons (Liberman, Seidman, McKenna, & Buffardi, 2011; Vitak, Crouse, & LaRose, 2011). Some have argued that abusing the Internet does not constitute a new problem for employers as employees had found innovative ways to loaf prior to the Internet (Block, 2001), but the Internet seems to exacerbate the loafing problem due to ease of access, the volume of online content, and types of activities that can be performed over the net that are not otherwise available (Phillips, 2006). The Academic and popular press has published many articles illustrating the negative implications of cyberloafing; perhaps none more captivating than the scandal at the Securities and Exchange Commission involving dozens of employees who spent sizable amounts of their workday viewing pornography (Simmons, 2010).

Research suggests that some cyberloafing can have positive implications in the workplace by reducing stress and adding variety to daily routines (Lim & Chen, 2009) but excessive use can result in lost time and reduced productivity (George, 1996; Griffiths, 2003) and cyberloafing tends to correlate with reduced workplace involvement (Liberman et al., 2011). As such, researchers have suggested that organizations should take a deterrence approach through the use of acceptable use policies (AUPs) for Internet-based applications (D'Arcy, Hovav & Galletta, 2009; Straub & Welke, 1998) coupled with Internet monitoring (detection) mechanisms (D'Arcy et al., 2009) to minimize time spent cyberloafing. Those researchers propose that the deterrence approach can be an effective way to reduce cyberloafing without blocking websites and impeding on the positive aspects of the Internet as AUPs aim to deter cyberloafing by including guidelines on appropriate Internet use, outlining potential sanctions for misuse, and coupling them with detection mechanisms that assist in the enforcement of the AUP (Ugrin & Pearson, 2008). But the effectiveness of the deterrence approach can be questioned considering that cyberloafing continues be a workplace problem and the results of existing research are inconsistent (e.g. D'Arcy et al., 2009; Herath & Rao, 2009; Li, Zhang, & Sarathy, 2010; Straub, 1990). For example, AUPs have been shown to influence abusive computer behavior in general by creating awareness of a policy and through their coupling policies with detection systems (Harrington, 1996). On the other hand, the threat of formal sanctions that are typically included in AUPs have actually been linked with increased Internet abuse (de Manrique Lara, 2006).

As researchers have investigated the effects of deterrence mechanisms on cyberloafing they have tended to treat all forms

* Corresponding author. Tel.: +1 785 532 5897.
E-mail addresses: jugrin@ksu.edu (J.C. Ugrin), jpearson@business.siu.edu (J. Michael Pearson).
[1] Tel.: +1 618 453 7802.

[2] Other names for cyberloafing in the literature are cyberslacking, non-work related computing or information systems misuse.

0747-5632/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chb.2012.11.005

of cyberloafing alike and have tended to assume that deterrence mechanisms will affect all types of cyberloafing in the same way. We propose that the inconsistencies highlighted above can be explained, in part, by the point that researchers have not examined the effects of the active enforcement of the sanctions within AUPs and have not observed the effects of deterrence mechanisms on specific types of cyberloafing. In accordance with those limitations, this research explores the effects sanctions, detection, and enforcement on a number of typical cyberloafing activities (viewing pornography, viewing traditional media, managing personal finances, personal shopping, personal emailing, and social networking) and illustrates how deterrence factors affect the various cyberloafing activities differently. By doing so, this research fills a gap in the academic literature and provides guidance as to the effectiveness of deterrence mechanisms that should be of value to practitioners.

The remainder of this paper is formatted as follows. First, we examine literature on deterring cyberloafing, discuss relevant theory and put forth a set of hypotheses. We then discuss the methodology and present the results. Finally, limitations and implications of the research are discussed and conclusions are drawn.

2. Hypotheses development

Traditionally, firms have attempted to mitigate cyberloafing by incorporating deterrence mechanisms to monitor and sanction inappropriate cyber behavior. In the literature, researchers tend to treat all types of cyber behavior alike, as if all cyberloafing violates rules and employees should assume such violations will result in consequences. However, to understand how individuals perceive the likelihood of consequences, attention must be given to individuals' personal views on whether or not the behavior in question is indeed perceived to be an unacceptable violation of organizational policies.

We propose that individuals consider how their Internet activities would fit into their own personal virtues and the norms of their workplace and society when deciding what types of activities constitute a violation. Beyond traits, moral decisions are a function of identification, e.g. whether or not the morality of a dilemma is identified (Rest, 1986). One would expect participants could be more apprehensive about cyberloafing if they recognized its effects on organizations. We propose that individuals discount the threat of potential consequences when behaviors are perceived to be acceptable. If abusive behaviors, as defined by an AUP, do not match those defined by employees, the AUP and the sanctions within become less effective and require additional measures like detection mechanisms and active enforcement to change attitudes and perceptions.

2.1. The deterrence model

A conception of the effects of AUPs on cyberloafing can be achieved through understanding General Deterrence Theory (GDT), a criminological theory dating back centuries, and is the foundation for a large body of research in criminal justice, ethics, and most recently, cyberloafing. GDT is based on an imposed regulatory model, emphasizing regulations that are placed on employees by organizations through the threat of sanctioning. GDT suggests that the threat of sanctions can modify employee actions when potential punishments are weighed against potential benefits of a specific behavior. When confronted with opportunities and related consequences, individuals are believed to be rational actors who weigh the costs versus rewards of taking an action (Williams & Hawkins, 1986). This perspective on ethical decision making relies on individuals seeking outcomes that benefit themselves.

GDT has three components that are proposed to have an influence on illicit behavior; sanctions, detection, and enforcement. The primary factor in the GDT model is sanctioning. Sanctions are effective to the extent they are deemed to be severe (D'Arcy et al., 2009; Ugrin & Odom, 2010). GDT is based on simple economic calculus where more punishment should equal more deterrence. In the context of cyberloafing, organizations with AUPs that threaten more severe consequences would theoretically see less cyberloafing. It is proposed that employees will be less likely to cyberloaf when the potential sanctions for cyberloafing are perceived to be more severe.

H1. Intentions to cyberloaf will be lower when the potential sanctions for cyberloafing are severe relative to when the potential sanctions are weak.

Although sanctions are important, GDT says that punishments must be imminent before they have an effect. Consequences that are perceived to be more likely will have greater deterrence. In other words, there must be a strong chance of being caught for a policy to be effective (Williams & Hawkins, 1986). In a study that examined the effects of monitoring non-work related computing in general, Urbaczewski and Jessup (2002) found that more monitoring activities resulted in less non-work related computing behavior. Likewise, Li et al. (2010) found that increased perceptions of detection as a result of monitoring can increase AUP compliance. However, Urbaczewski and Jessup's (2002) and Li et al.'s (2010) studies only focused on the main effects of deterrence mechanisms, not accounting for any interaction between potential sanctions and monitoring activities. GDT suggests that any actions that increase the likelihood that one will be punished, such as monitoring activities that result in detection, will make the threat of potential sanctions more effectual (Nagin & Pogarsky, 2001). In the context of cyberloafing, the presence of such mechanisms increases the potential to be caught, making punishment more likely and resulting in a positive interaction between potential sanctions for cyberloafing and monitoring mechanisms.

A question that can be raised is, "if organizations introduce potential sanctions for cyberloafing and mechanisms that can detect Internet activities, will the threat of sanctions coupled with detection mechanisms reduce cyberloafing without active enforcement?" In other words, the perceived certainty of sanctions can be increased if people are aware that they are enforced after people are caught. D'Arcy et al. (2009) found that the certainty of sanctions can influence cyberloafing and Lee and Lee (2002) found that individuals are less likely to use company provided computers for inappropriate behavior when the individuals were aware of others being punished. But those papers did not test if it was the awareness of enforcement that deterred individuals or the interactive effects between enforcement, detection, and the potential consequences. In unrelated contexts, studies by Simpson and Koper (1992) and Ugrin and Odom (2010) examined the interactive effects of enforcement and sanctions. Simpson and Koper (1992) examined the impact of past guilty verdicts on reducing antitrust violations by corporations, finding that awareness of enforcement resulted in fewer violations and Ugrin and Odom (2010) examined the impact of the enforcement of sanctions for committing financial fraud on financial manager's attitudes about committing fraud, finding a three-way interaction between sanctions and enforcement when detection mechanisms were in place. Although these studies are contextually unrelated and the Simpson and Koper study is at the firm level, they lend support for enforcement as a moderating factor in the GDT model. Similarly, we expect that the effect of potential sanctions on cyberloafing will be moderated by employees' awareness of sanctions being enforced. We propose that the effects of potential punishment and detection will be

moderated by enforcement. Punishment will be a strong deterrent if individuals expect to be caught and expect that the potential punishment will indeed be handed down.

Even with deterrence mechanisms in place and active enforcement, employees' ethical values have a significant role in the ultimate effectiveness of the mechanisms at deterring behavior a priori. Tyler and Blader (2005, p. 1149) state, "employees' ethical values play (a role) in motivating rule following, and in particular those ethical values that are related to – and developed in the course of interactions – with their work organizations" (Tyler & Blader, 2005, p. 1149). Research suggests that when individuals feel their organization is being managed with a sense of ethics that are in line with their own, they will typically behave in accordance with the policies and rules of the organization (King & Lenox, 2000; Tyler & Blader, 2005). That should hold true for Internet usage and the alignment between employee feelings toward cyberloafing and employers' rules and policies. Research has shown in a variety of contexts that personal feelings can have a moderating effect on the impact of deterrence factors on illicit behaviors, showing that deterrence factors are more effectual on more acceptable behaviors (Li et al., 2010; Paternoster & Simpson, 1996) and are more effectual on individuals who are less morally restrained (D'Arcy et al., 2009).[3] In the context of cyberloafing, where the effect of mechanisms like sanctions and detection have been shown to be effective deterrents in some studies but not in others, it seems difficult to rectify conflicting results in existing studies without examining various types of cyberloafing individually. For example, the literature (e.g. D'Arcy et al., 2009; de Manrique Lara, 2006; Li et al., 2010) tends to use either single scales or composite scores to test Internet usage intentions in general, not intentions to use the Internet for specific behaviors like sending personal emails or using the Internet to view pornography. That distinction is critical as research has shown that many employees feel that some types of Internet usage at work should be for both work related and non-work related activities (Whitty, 2004), potentially creating mis-alignment between employer and employee values and feelings of what is acceptable in the workplace and what is not. If that is the case, deterrence mechanisms must be in place if an employer aims to reduce Internet activities that are deemed acceptable by employees.

Taken as a whole, we have proposed that the threat of sanctions can deter cyberloafing but sanctions are more effectual when accompanied by detection mechanisms, active enforcement, and on activities that are initially deemed acceptable in the workplace.

H2. The effect of potential sanctions on cyberloafing will be moderated by an increased likelihood of detection and evidence of past enforcement for less abusive behaviors and not for more abusive behaviors.

The research model is presented in Fig. 1.

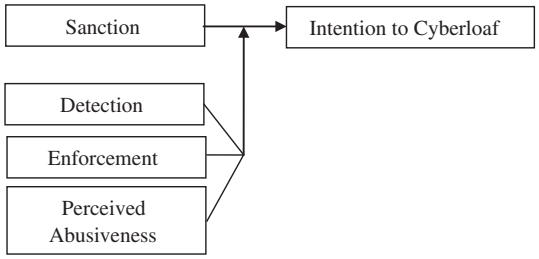

Fig. 1. Deterrence model.

3. Methodology

3.1. Participants

Data was collected from 156 individuals. Data from six individuals was removed due to failure to provide complete information or failure to accurately answer manipulation check items that tested the diligence with which they participated. The resultant sample included 69 business students at two large public universities in the United States, and 81 employees representing three firms in the United States, a manufacturing firm, a bank, and an educational institution. Most of the students (42) were also employed. The sample's mean age was 26.63 with an average of 7.40 years of work experience (Column A in Table 1). Tests of demographics across treatment conditions and perceptions of the abusiveness of various types of cyberloafing revealed that participants' with differing levels of self-control (the variable is discussed in more detail below) was not evenly distributed across treatment conditions (Column B in Table 1). In addition, participants' gender, age and work experience were correlated ($P < .05$) with their perception as to the deviance of social networking in the workplace (Column C in Table 1). Males, older participants, and participants with more work experience perceived social networking to be more abusive. Also, those who worked in management perceived viewing traditional media online in the workplace and individuals with more self-control perceived viewing pornography online in the workplace to be more abusive (Column C in Table 1). Gender, Age, and years of work experience were controlled in hypotheses tests involving social networking. Status as a manager was controlled in hypotheses tests involving traditional media and self-control was controlled in all hypotheses tests.

3.2. Procedures

Participants were administered an experimental survey. Each individual was randomly assigned one scenario that manipulated information related to three facets of deterrence – potential sanctions for cyberloafing, detection mechanisms designed to catch cyberloafing, and past enforcement of sanctions on those that were previously caught cyberloafing. After considering the potential sanctions, potential detection, and past enforcement, participants were asked to respond to several manipulation checks and asked to indicate the likelihood they would engage in six types of cyberloafing activities. Additionally, participants were asked to rate how abusive they perceived each type of cyberloafing to be and were asked to respond to a number of other items that aimed to help explain the results or measure potential confounding factors. Finally, participants were asked to self-report demographic information.

3.3. Measures

3.3.1. Dependent variable

The dependent variables were measured across six types of cyberloafing; Online Shopping (SHOPPING), Money Management (INVEST), Emailing (EMAIL), Social Networking (SOCIALMEDIA), Viewing Online Pornography (PORN), and Viewing Traditional Online Media (MEDIA). Individuals' intentions to participate in each type of cyberloafing were measured with Likert scaled items asking participants the likelihood that others that work for that company would use the company's Internet resources to engage in personal shopping, managing personal finances, social networking, sending personal emails, viewing pornography, or watching or reading the news (Appendix A). The reason for eliciting participants' perceptions about referent others (coworkers) is that responses to ethical decisions are often biased by a "halo effect" where individuals do not reveal their true intentions when they are asked directly about

[3] In a limited post-hoc analysis, D'Arcy et al. (2009), found that moral commitment moderates the effects of sanctions on intentions to misuse the Internet.

Table 1
Sample characteristics (n = 150).

Demographic variable	Column A	Column B	Column C Correlation between demographic variables and types of behavior					
	Total	Group diff. across treatments for sanction, detection and enforcement	Shopping[c]	Invest[c]	Social media[c]	Email[c]	Porn[c]	Media[c]
Gender: Female (Male)	70 (80)	$P > .05$[b]	.034	.122	.187[d]	−.067	.121	.142
Age: Mean (Std. Dev)	26.63 (8.10)	$P > .05$[a]	.043	−.131	.173[d]	−.088	.102	.069
Employed: Yes (No)	27 (123)	$P > .05$[b]	−.134	−.116	−.035	−.064	.098	.022
Years work experience: Mean (Std. Dev)	7.40 (6.64)	$P > .05$[a]	.024	−.096	.204[d]	−.075	.165	.073
Work in management: Yes (No)	35 (115)	$P > .05$[b]	−.010	.091	−.156	−.155	−.021	.217[d]
Responsibility denial: (RESPDEN): Mean (Std. Dev)	80.45 (6.30)	$P > .05$[a]	.139	−.010	−.092	.097	.116	−.072
Self-control (SELFCONT): Mean (Std. Dev)	57.36 (9.61)	$P < .05$[a]	.020	−.042	−.004	−.129	−.173[d]	−.006
Cyberloafing harms others (HARM): Mean (Std. Dev)	2.13 (.83)	$P > .05$[a]	.042	.024	−.105	−.140	.043	.008
Habit: Mean (Std. Dev)	2.89 (1.32)	$P > .05$[a]	−.043	.007	.020	−.101	−.006	−.131

[a] ANOVA: significance of the mean difference between treatment groups. Individual treatment means not tabulated.
[b] Chi-Square: significance of the frequency differences between treatment groups. Frequencies for individual treatment conditions are not tabulated.
[c] Correlation between demographic variable and perception of the abusiveness of the type of cyberloafing behavior.
[d] $P < .05$.

Table 2
Mean abusiveness ratings.

Cyberloafing activity	Subset for alpha = 0.05			
	1	2	3	4
EMAIL (personal email)[c]	30.8[c]			
INVEST (personal money management)[c]		47.9[c]		
SOCIALMEDIA (Social networking)[c]		54.2[c]		
MEDIA (Viewing traditional media)[c]		54.5[c]		
SHOPPING (personal shopping)[c]			61.9[c]	
PORN (Viewing Pornography)[c]				96.8[c]

[a] Mean abusiveness ratings for groups in homogeneous subsets are displayed ($P < .05$).
[b] Homogeneous subsets computed using Tukey HSD.
[c] 0 = Not abusive; 100 = abusive.
[d] Overall mean = 57.7; Overall Std. Dev. = 29.2.
[e] N = 150.

actions that may have potential social ramifications, but project them on a referent other when asked how the other would respond (Clement & Krueger, 2000; Mikulineer & Horesh, 1999; Ruvolo & Fabin, 1999; Smith, 1997).[4]

3.3.2. Independent variables

The deterrence mechanisms – sanctions (SANCTION), detection (DETECTION), and enforcement (ENFORCEMENT) – were manipulated in the experimental survey. There were two levels of each variable. The variables were manipulated using the following statements:

> Imagine that you work for a company and you are aware of the following information related to computer deterrence and security measures at that company. Consider the three measures presented below and then answer the following questions about how you would use the Internet at that organization.
> *– The company's Internet use policy CONTAINS a statement stating that you will be FIRED (or VERBALLY REPRIMANDED) if you abuse the Internet at work.*
> *– The company EMPLOYS (or DOES NOT EMPLOY) security detection systems capable of monitoring your Internet activity in the workplace.*
> *– Others within the organization that have been caught abusing the Internet at work HAVE (or HAVE NOT) been punished in accordance with the sanction listed above.*

As mentioned, three manipulation checks items ensured participants' understood the manipulations. The manipulation checks were: "the company's Internet use policy states that you can be fired (verbally reprimanded) for abusing the Internet in the workplace", "the company employs (does not employ) a system to monitor Internet activity" and "the company has (has not) punished others for abusing the Internet in the workplace."

To assess how abusive participants' perceived the six types of cyberloafing, they were asked to rate the six different types of cyberloafing on a scales that ranged from not abusive (0) to very abusive (100) (ABUSIVENESS) (see Appendix B for the items).

3.3.3. Potential covariates and additional measures

Various factors could systematically influence results and we collected measures to ensure they were evenly distributed across treatment conditions and test if they correlated significantly with the dependent variables. Individual's inherent levels of self-control (SELFCONT) (individuals low in self-control are less likely to control the urge to engage in illicit behavior) and responsibility denial (RESPDEN) (individuals that rate high in responsibility denial tend

[4] Participants were also asked how they would behave directly but only the referent data was used in the analyses.

Table 3
ANOVA results across treatment conditions. Test of between subjects effects (intercept and covariates omitted).

Effect	Dependent variable	Type III sum of squares	df	Mean square	*F*	Sig.
SANCTION (S)	Shopping[b]	20.570	1	20.570	9.985	.002
	Invest[c]	47.590	1	47.590	26.352	.000
	SocialMedia[d]	17.491	1	17.491	8.981	.003
	Email[e]	51.887	1	51.887	24.381	.000
	Porn[f]	.023	1	.023	.157	.693
	Media[g]	10.553	1	10.553	4.855	.029
DETECTION (D)	Shopping	14.517	1	14.517	7.047	.009
	Invest	9.558	1	9.558	5.292	.023
	SocialMedia	52.478	1	52.478	26.946	.000
	Email	46.395	1	46.395	21.801	.000
	Porn	.775	1	.775	5.165	.025
	Media	45.883	1	45.883	21.110	.000
ENFORCEMENT (E)	Shopping	.076	1	.76	.037	.848
	Invest	17.459	1	17.459	9.667	.002
	SocialMedia	17.700	1	17.700	9.089	.003
	Email	5.592	1	5.592	2.628	.107
	Porn	.014	1	.014	.094	.760
	Media	24.931	1	24.931	11.470	.001
ABUSIVENESS (A)	Shopping	2.459	1	2.459	1.194	.277
	Invest	32.318	1	32.318	17.895	.000
	SocialMedia	.106	1	.106	.054	.816
	Email	.314	1	.314	.148	.701
	Porn	.031	1	.031	.207	.650
	Media	3.785	1	3.785	1.742	.189
S × D × E × A	Shopping	13.603	11	1.237	.600	.826
	Invest	25.951	11	2.359	1.306	.228
	SocialMedia	35.779	11	3.253	1.670	.087
	Email	39.971	11	3.634	1.707	.078
	Porn	2.555	11	.232	1.549	.122
	Media	20.744	11	1.886	.868	.574

[a] $N = 150$.
[b] Adj. R squared = .081.
[c] Adj. R squared = .312.
[d] Adj. R squared = .294 (Gender ($P < .10$) and Gender ($P < .05$) are significant in the model).
[e] Adj. R squared = .289.
[f] Adj. R squared = .123 (Self-control ($P < .10$) is significant in the model).
[g] Adj. R squared = .224 (Having served as a manager is significant in the model ($P < .05$).

to depersonalize illicit acts and place responsibility on others) could influence the outcomes. Self-control was be measured by a 24-item 5-point Likert type scale (Grasmick, Tittle, Bursik, & Arneklev, 1993; Nagin & Paternoster, 1993) and responsibility denial was measured by a 28-item 5-point Likert type scale (Harland, Staats, & Wilke, 2007; Harrington, 1996; Schwartz, 1973).

Beyond traits, moral decisions are a function of identification, e.g. whether or not the morality of a dilemma is identified (Rest, 1986). One would expect participants could be more apprehensive about cyberloafing if they recognized its effects on organizations. To measure that perception, participants were asked if "using the Internet for personal purposes at work harms firms?" (HARM) (1 = does not harm and 7 = is very harmful). Internet use and misuse has also been shown to be habitual (Woon & Pee, 2007). This was assessed by a single Likert scaled item that states "have you used the Internet or Internet resources for personal purposes during work time" (HABIT) (1 = never and 7 = often).

4. Results

4.1. Preliminary analysis

In a preliminary analysis, we compared participants' perceptions on the abusiveness of each type of cyberloafing. Participants felt that viewing pornography (PORN) was the most abusive whereas personal emailing (EMAIL) was the least abusive followed by personal money management (INVEST), social networking (SOCIALMEDIA), viewing traditional online media (MEDIA), and personal shopping (SHOPPING). A summary of the ratings relative to one another are presented in Table 2.

4.2. Hypotheses tests

To test the hypotheses, six individual ANOVAs were computed. Each of the independent variables (SANCTION, DETECTION, ENFORCEMENT, and ABUSIVENESS) was included in the models along with a four-way interaction term between the variables and other relevant control variables. Data for SANCTION, DETECTION, and ENFORCEMENT were manipulated at two levels. The measure for ABUSIVENESS was dichotomized using a mean split.[5] The ANOVA results are presented in Table 3. The means and standard deviations for participants' responses to the intention to cyberloaf measures are presented in Table 4. A correlation matrix for the independent and dependent variables is presented in Appendix C.

Recall, hypothesis one stated, "Intentions to cyberloaf will be lower when the potential sanctions for cyberloafing are severe relative to when the potential sanctions are weak." In the ANOVA results, there are significant main effects for SANCTION (the threat of being fired or receiving a verbal reprimand) across all types of cyberloafing ($P < .05$) except for viewing pornography (PORN) (Table 3). Further analyses of the mean responses to the dependent variable

[5] A median split could not be used to dichotomize perceived abusiveness of viewing pornography due to the skew of the data thus a mean split was performed. A median split could be performed on participants' perceptions of other types of cyberloafing but results were not different than the results with a mean split. As a matter of consistency a mean split was performed for all data.

Table 4
Likelihood to cyberloaf per treatment condition.

		Shopping potential sanction		Invest potential sanction		Social media potential sanction		Email potential sanction		Porn potential sanction		Media potential sanction	
		Fire	Reprimand	Fire	Reprimand	Fire	Reprimand	Fire	Reprimand	Fire	Reprimand	Fire	Reprimand
High abusiveness													
Enforcement	Detection (High probability)	2.000 (1.109) {14}	2.429 (1.134) {7}	1.400 (.516){10}	1.727 (.786) {11}	2.182 (1.079) {11}	1.714 (.951) {7}	3.083 (.900) {12}	2.778 (.972) {9}	1.000 (.000) {14}	1.000 (.000) {15}	2.200 (.789) {10}	3.000 (1.205) {4}
	Detection (Low probability)	2.833 (1.115) {12}	2.286 (1.254) {7}	2.143(1.574) {7}	2.750 (1.603){12}	3.010 (1.604) {8}	3.000 (1.549) {6}	5.125 (1.642) {8}	4.800 (2.280) {5}	1.067 (.258) {15}	1.143 (.363) {14}	3.300 (1.703) {10}	4.778 (1.563) {9}
No enforcement	Detection (High probability)	2.833 (1.403) {12}	2.769 (1.301) {13}	2.800 (1.082) {15}	3.769 (1.012){13}	2.765 (1.300) {17}	2.700 (1.337) {10}	4.810 (2.098) {10}	5.625 (1.061) {8}	1.278 (.461) {18}	1.000 (.000) {18}	3.177 (1.334) {17}	3.583 (1.443) {12}
	Detection (Low probability)	3.667 (1.366) {6}	4.000 (1.673) {11}	2.200 (1.229) {10}	4.462 (1.664) {13}	3.636 (2.063) {11}	5.000 (1.871) {5}	5.500 (2.121) {2}	6.400 (.548) {5}	1.118 (.485) {17}	1.438 (.727) {16}	3.000 (1.155) {4}	6.000 (-) {1}
Enforcement	Detection (High probability)	2.333 (1.155) {3}	2.083 (1.311) {12}	2.286 (.952) {7}	2.750 (1.753) {8}	1.500 (.837) {6}	2.667 (1.557) {12}	2.800 (.837) {5}	3.800 (1.476) {10}	1.000 (.000) {3}	1.000 (.000) {4}	1.571 (.535) {7}	2.600 (1.121) {15}
Low abusiveness													
	Detection (Low probability)	3.333 (1.966) {6}	3.417 (1.782) {12}	3.000 (1.897) {11}	4.286 (.756) {7}	3.300 (1.418) {10}	3.000 (1.683) {13}	5.500 (1.080) {10}	5.286 (1.729) {14}	1.667 (.577) {3}	1.600 (.548) {5}	3.875 (1.458){8}	3.800 (2.098) {10}
No enforcement	Detection (High probability)	3.750 (1.581) {8}	3.000 (1.549) {6}	4.400 (1.817) {5}	3.667 (1.862) {6}	1.667 (1.155) {3}	3.111 (.928) {9}	4.900 (1.792) {10}	5.546 (.820) {11}	1.000 (.000) {2}	1.000 (-) {1}	3.000 (2.646) {3}	3.429 (1.813) {7}
	Detection (Low probability)	3.385 (1.260) {13}	3.750 (1.832) {8}	4.000 (1.225) {9}	4.844 (1.169) {6}	2.875 (1.356) {8}	5.214 (1.424) {14}	5.059 (1.638) {17}	6.143 (1.351) {14}	1.000 (.000) {2}	1.333 (.577) {3}	3.733 (1.752) {15}	4.944 (1.434) {18}

*Mean (Std. Dev.){n}.

measures (Table 4) reveal that when confronted with the threat of being fired, the participants are less likely to cyberloaf compared to being confronted with the threat of a verbal reprimand, with the exception of PORN. These findings support hypothesis one.

Hypothesis two stated, "The effect of potential sanctions on cyberloafing will be moderated by an increased likelihood of detection and evidence of past enforcement for less abusive behaviors". This would be evidenced by a significant interaction term between SANCTION, DETECTION, ENFORCEMENT, and ABUSIVENESS where deterrence mechanisms are more effectual when a behavior is perceived to be less abusive. The results reveal marginally significant interaction terms for SOCIALMEDIA and EMAIL (Table 3). Further analysis of the mean responses to SOCIALMEDIA and EMAIL across treatment conditions reveal that responses to SOCIALMEDIA and EMAIL tend to be lower when the threat of SANCTION includes jail, DETECTION is more likely, participants are aware of ENFORCEMENT, and ABUSIVENESS is perceived to be low (Table 4). This suggests that when using social media or sending personal emails in the workplace is not perceived to be abusive in nature, detection mechanisms and active enforcement are needed if those behaviors are to be influenced. These findings support hypothesis two for SOCIALMEDIA and EMAIL. The findings were not significant for the other forms of cyberloafing.

Considering that dichotomizing the ABUSIVENESS measures eliminated some variability and may account for only finding significance for hypothesis two for SOCIALMEDIA and EMAIL, the individual ANOVA tests were performed again for SHOPPING, INVEST, and MEDIA[6] using only data from participants that rated those factors more than one standard deviation away from the mean ABUSIVENESS rating for each behavior respectively. In those analyses we did not find any significant four-way interaction for SHOPPING, INVEST, or MEDIA (all $P > .10$) (not tabulated). Overall, the findings partially support hypothesis two.

5. Discussion and conclusion

The results shed more light on how individuals decide to engage in using the Internet and how individuals decide to incorporate deterrence mechanisms into their decision process beyond the existing research. The possibility of being fired influenced the likelihood that participants would engage in all types of cyberloafing (except viewing pornography). However, we found that personal emailing and viewing social media were deterred when the possibility of getting fired was coupled with a detection mechanism, knowledge of active enforcement in the past, and a perception that emailing is acceptable.

Although the results are not identical for all types of cyberloafing they do suggest that more mechanisms are required to deter the behaviors that were deemed more acceptable. These results may provide an explanation for the disparate findings among existing deterrence based studies which tend to treat all types of cyberloafing similarly. From a theoretical point of view, these findings tend to bring together theories on ethical decision making rather than supplant or refute them. By showing that imposed deterrence factors tend to be more effective at reducing less deviant behaviors our findings are consistent with both a lower order approach to ethical decision making predicated on punishment and obedience (classical deterrence theory) and an approach based on higher order reasoning predicated on the recognition of right and wrong (e.g. the Rest (1986) model) and the use of that recognition to guide action. It is logical to conjecture from the results presented in this paper that recognition of right and wrong (abusiveness) guides the anticipation and effect of sanctions and consequences.

[6] The analysis could not be performed on PORN due to the skew of the data.

Thus actions are influenced by both lower and higher order reasoning. Additionally, where others have shown that moral judgment leads to intentions to act (e.g. Haines & Leonard, 2007) we show that moral judgment (or perceived abusiveness) works in conjunction with other factors in influencing intentions to act.

From a practical perspective, the findings suggest that the effectiveness of imposed deterrence mechanisms (e.g. AUPs or Internet monitoring) is contingent on the behavior and individual feelings and perceptions about the behavior. It is reasonable to conclude from our findings that AUPs and Internet monitoring will be relatively ineffective at reducing behaviors like personal emailing and social networking unless employees know about of others who have been caught and punished severely. Perhaps this does little to solve the quandary that employers face when trying to balance how much deterrence to impose with employee morale and other costs; in fact the findings seem to exacerbate what seems like a catch-22. This is a limitation of the study that should be addressed by future research. For example, we do not account for negative affect that can be a result of the use of deterrence mechanisms and detection and research has shown that simply introducing these types of deterrence methods can create employee strife (de Manrique Lara, 2006). In addition to the negative affect sanctions and detection can have on employee morale, detection also creates issues with privacy. Furthermore, recent literature has focused on the positive psychological aspects of personal Internet usage in the workplace such as reduced stress and negative emotions (e.g. Lim & Chen, 2009). Future research should aim to find a balance between deterring abusive Internet usage without interfering with the positive effects of using the Internet.

In addition to imposing additional deterrence mechanisms, firms may also influence behaviors by changing perceptions about what behaviors are or are not acceptable. Perhaps this could happen through continued enforcement. Failure to enforce may actually exacerbate problems by supporting and advancing existing perceptions that behavior like personal emailing or social networking are acceptable. Future researchers may want to explore how enforcement and perceptions about the egregiousness of different types of cyberloafing interact with one another. Structuration theory could provide the foundation. It suggests that social structures and norms are a function of the repetitive enactment of processes and behaviors and changing behaviors will change norms and revise beliefs. We should point out however, that even if detection and enforcement are important, changes in technology will make them hard to implement. For example, many of the activities tested here can be performed on smart phones with Internet access or other personal Internet devices, giving employees an ability to circumvent detection.

Other limitations are inherent in our methodology. For example, survey based experiments measuring behavioral intentions are commonly used in social science and ethics research, but intentions are not actual behavior. Other factors could ultimately influence whether or not individuals act as intended such as perceived control mechanisms like access to websites and office location and privacy (for instance, if the employee works in an office or a cubicle). The most effective way to overcome these types of limitations and examine these issues would be to track actual activities in the workplace.

Finally, future research could incorporate factors that can further explain how intentions are arrived at and how actions are rationalized. One factor is framing. It would be interesting to examine if framing AUPs in different ways have different effects on intentions and behaviors.

In summary, this research has provided a more comprehensive look at deterring cyberloafing than has been done before. It has shown that cyberloafing in the workplace is a complex issue that is contingent on the situation and the individual engaging in the activity. It has filled a gap in the academic literature and provided more information for practitioners about the potential effects of their deterrence activities.

Appendix A. Dependent variable measures

Considering the information in the scenario, ***what is the likelihood that others that work for that company*** would use the company's Internet resources to do the following activities: Please circle one answer for each activity:

Personal shopping	1 Not likely	2	3	4	5	6 7 Highly likely
Manage personal finances	1 Not likely	2	3	4	5	6 7 Highly likely
Social network (e.g. Facebook)	1 Not likely	2	3	4	5	6 7 Highly likely
Send personal emails	1 Not likely	2	3	4	5	6 7 Highly likely
View pornography	1 Not likely	2	3	4	5	6 7 Highly likely
Watch or read the news	1 Not likely	2	3	4	5	6 7 Highly likely

Appendix B. (Perceptions of the relative abusiveness of each type of cyberloafing)

Please rate how you feel about the relative abusiveness of performing the following activities on the Internet while at work by **marking a slash on the scale**.

Personal shopping	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior
Managing personal finances	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior
Social networking	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior
Personal emailing	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior
Viewing pornography	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior
Watching or reading news	0 Not abusive (bad) behavior	25	50	75	100 Very abusive (bad) behavior

Appendix C. Correlation matrix for the variables used in the tests of the hypotheses

	SHOPPING	INVEST	SOCIAL-MEDIA	EMAIL	PORN	MEDIA	SANCTION	DETECTION	ENFORCEMENT	ABUSIVENESS SHOPPING	ABUSIVENESS INVEST	ABUSIVENESS SOCIALMEDIA	ABUSIVENESS EMAIL	ABUSIVENESS PORN	ABUSIVENESS MEDIA
SHOPPING	1														
INVEST	.643[a]	1													
SOCIALMEDIA	.553[a]	.454[a]	1												
EMAIL	.568[a]	.517[a]	.526[a]	1											
PORN	.204[b]	.149[b]	.257[a]	.063	1										
MEDIA	.503[a]	.585[a]	.566[a]	.585[a]	.119	1									
SANCTION	−.260[a]	−.354[a]	−.260[a]	−.350[a]	−.170[b]	.200[b]	1								
DETECTION	−.250[a]	−.206[b]	−.366[a]	−.356[a]	−.230[a]	−.376[a]	−.013	1							
ENFORCEMENT	−.009	−.231[a]	−.172[b]	−.133	.030	−.236[c]	−.027	0	1						
ABUSIVENESS SHOPPING	−.151[c]	−.149[c]	−.031	−.032	−.064	−.077	−.116	.123	.186[b]	1					
ABUSIVENESS INVEST	−.253[a]	−.215[b]	−.090	−.147[c]	−.062	−.192[b]	.006	.204[b]	−.057	.310[a]	1				
ABUSIVENESS SOCIALMEDIA	−.149[c]	−.156[c]	−.157[c]	.113	−.205[b]	−.139	−.067	.207[b]	.171	.277[a]	.272[a]	1			
ABUSIVENESS EMAIL	−.273[a]	−.272[a]	−.237[a]	−.167[c]	−.167[c]	−.303[a]	.042	.340[a]	.075	.286[a]	.470[a]	.369[a]	1		
ABUSIVENESS PORN	−.001	−.062	−.075	.102	−.260[a]	−.001	.003	.168[c]	.143	.265[a]	.121[c]	.256[c]	.059	1	
ABUSIVENESS MEDIA	−.187[b]	−.236[a]	−.176[b]	−.047	−.227[b]	−.185[b]	.059	.275[a]	.244	.353[a]	.357[a]	.426[a]	.412[a]	.181[b]	1

[a] Correlation is significant at the 0.01 level (2-tailed).
[b] Correlation is significant at the 0.05 level (2-tailed).
[c] Correlation is significant at the 0.10 level (2-tailed).
[d] $N = 150$ for full table.

Appendix D. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.chb.2012.11.005.

References

Blanchard, A., & Henle, C. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior, 24*(3), 1067–1084.

Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics, 33*(3), 225–232.

Clement, R., & Krueger, J. (2000). The primacy of self-referent information in perceptions of social consensus. *British Journal of Social Psychology, 39*(2), 279–299.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

de Manrique Lara, J. (2006). Fear in organizations: Does intimidation by formal punishment mediate the relationship between interactional justice and workplace Internet deviance. *Journal of Managerial Psychology, 21*, 580–592.

George, J. (1996). Computer-based monitoring: common perceptions and empirical results. *MIS Quarterly, 20*(9), 459–480.

Grasmick, H., Tittle, C., Bursik, R., & Arneklev, B. (1993). Testing the core implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency, 30*(5), 5–29.

Griffiths, M. (2003). Internet abuse in the workplace: Issues and concerns for employers and employment counselors. *Journal of Employment Counseling, 40*(2), 87–96.

Haines, R., & Leonard, L. (2007). Situational influences on ethical decision making in an IT context. *Information and Management, 44*, 313–320.

Harland, P., Staats, H., & Wilke, H. (2007). Situational and personality factors as direct or personal norms mediated predictors of pro-environmental behavior: Questions derived from norm-activation theory. *Basic and Applied Social Psychology, 29*(4), 323–334.

Harrington, S. (1996). The effect of code of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257–278.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

King, A., & Lenox, M. (2000). Industry self-regulation without sanctions. *Academy of Management Journal, 36*, 502–526.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57–63.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*, 635–645.

Liberman, B., Seidman, G., McKenna, K., & Buffardi, L. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior, 27*, 2192–2199.

Lim, V., & Chen, D. (2009). Cyberloafing at the workplace: Gain or drain? *Behaviour and Information Technology, 90*(3), 1–11.

Lim, V., Teo, T., & Loo, G. (2002). How do I loaf here: Let me count the ways. *Communications of the ACM, 41*(1), 66–70.

Mikulineer, M., & Horesh, N. (1999). Adult attachment style and the perception of others: The role of projective mechanisms. *Journal of Personality and Social Psychology, 79*(6), 1022–1034.

Nagin, D., & Paternoster, R. (1993). Enduring individual differences in rational choice theories of crime. *Law and Society Review, 27*(3), 467–496.

Nagin, D., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology, 39*(4), 865–891.

Paternoster, R., & Simpson, S. (1996). Sanctions threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review, 30*(3), 549–584.

Phillips, J. (2006). The psychology of Internet use and misuse. *Advances in Management Information Systems, 7*, 41–62.

Rest, J. (1986). *Moral development: Advances in theory and research*. New York: Praeger.

Ruvolo, A., & Fabin, J. (1999). Two of a kind: Perceptions of own and partner's attachment characteristics. *Personal Relationships, 6*(1), 57–79.

Schwartz, S. (1973). Normative explanations of helping behavior: A critique, proposal, and empirical test. *Journal of Experimental Social Psychology, 9*, 349–364.

Simpson, S., & Koper, C. (1992). Deterring corporate crime. *Criminology, 30*(3), 347–375.

Smith, E. (1997). Private selves and shared meanings: Or forgive us for our prejections as we forgive those who project onto us. *Psychodynamic Counseling, 3*(2), 117–131.

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

Straub, D., & Welke, J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Tyler, T., & Blader, S. (2005). Can businesses effectively regulate employee conduct?: The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143–1158.

Ugrin, J., & Odom, M. (2010). Exploring the Sarbanes–Oxley act and intentions to commit financial statement fraud: A general deterrence perspective. *Journal of Accounting and Public Policy, 29*(5), 439–458.

Ugrin, J., & Pearson, J. (2008). Exploring Internet abuse in the workplace: How can we maximize deterrence efforts? *Review of Business, 28*(2), 29–40.

Urbaczewski, A., & Jessup, L. (2002). Does electronic monitoring of employee Internet usage work? *Communications of the ACM, 45*(1), 80–83.

Vitak, J., Crouse, J., & LaRose,, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior, 27*(5), 1751–1759.

Whitty, M. (2004). Should filtering software be utilized in the workplace? Australian employees' attitudes towards internet usage and surveillance of the internet in the workplace. *Surveillance and Society, 2*(1), 39–54.

Whitty, M., & Carr, A. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace. *Computers in Human Behavior, 22*, 235–250.

Williams, K., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review, 20*(4), 545–572.

Woon, I., & Pee, L. (2007). *Behavioral factors affecting Internet abuse in the workplace – An empirical investigation*. Proceedings of the Third Annual Workshop on HCI Research in MIS.

Simmons, C. (2010). GOP ramps up attacks on SEC over porn surfing. *USA Today*. <http://www.usatoday.com/money/companies/regulation/2010-04-22-sec-employees-porn_N.htm?POE=click-refer>.