Bringing cyber loafers back on the right track

Pablo Zoghbi-Manrique-de-Lara and Arístides Olivares-Mesa
Department of Economics and Management,
University of Las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Spain

Received 27 January 2010
Revised 29 March 2010,
4 April 2010
Accepted 18 April 2010

Abstract

Purpose – Despite the use in companies of policy and control mechanisms to tackle cyberloafing, these practices are still popular among employees. The purpose of this paper is to suggest that control systems alone are unable to deter cyberloafing because they are eventually perceived as a sort of "ineffectual dog that may bark a lot, but ultimately does not bite." Instead, control systems are only expected to deter cyberloafing if employees view them as leading to punitive consequences.

Design/methodology/approach – First, given the easy visibility of cyberloafing activities, the paper proposes a design for control systems that not only includes perceptions of organizational control (monitoring), but also perceptions of the supervisor's physical proximity (proximity). Data are collected from university administration and services personnel, whose main working tool is the computer. They all have internet access and individual e-mail, a stable physical location at work, and a supervisor. Multiple hierarchical regressions are used to test whether in reality proximity and monitoring are unable to decrease cyberloafing unless they interact together with employees' fear of formal punishment (punishment).

Findings – Only by interacting together and with punishment are proximity and monitoring able to deter cyber loafers from engaging in cyberloafing.

Research limitations/implications – The study could suffer from mono-method/source bias, and the university that supplied the sample has certain job conditions similar to those of the public sector, thus raising concerns about the generalizability of the results.

Practical implications – The results suggest that organizational managers should not only ensure that control systems are able to discover incidents and identify the perpetrators, but they should also follow them up with punitive consequences. Only if control systems are implemented together with punishment are they effective in eliciting perceived certainty among cyber loafers of being caught and sanctioned, and hence in "bringing them back on the right track."

Originality/value – Despite the extensive use of control systems to deter cyberloafing, there are no previous empirical studies that have examined and supported the negative interacting effects of proximity, monitoring, and punishment on cyberloafing.

Keywords Employee behaviour, Human resource management, Internet, Organizational culture, System monitoring, Punishment

Paper type Research paper

1. Introduction

The ubiquity of information and communication technologies in the workplace is increasingly apparent. One cyber activity that has recently received a lot of attention among organizational scholars is cyberloafing (also called cyberslacking). Lim (2002, p. 677) defines cyberloafing as:

> [...] any voluntary act of employees' using their companies' internet access during office hours to surf non job-related Web sites for personal purposes and to check (including receiving and sending) personal e-mail.

Industrial Management & Data Systems
Vol. 110 No. 7, 2010
pp. 1038-1053
© Emerald Group Publishing Limited
0263-5577
DOI 10.1108/02635571011069095

Cyberloafing is a prevalent and costly problem for organizations. Malachowski (2005) refers to this inappropriate use of the internet as the most common way for employees to waste time at work. Current estimates range from a little over three hours per week (Greenfield and Davis, 2002) to 2.5 hours per day (Mills *et al.*, 2001). In addition, cyberloafing can cause problems in the information system's security and general proper functioning, such as bandwidth clogging, spyware infection, and task postponement (Levoie and Pychyl, 2001; Sipior and Ward, 2002). Illegal or unethical behaviors derived from the abuse of these technologies can also harm employees and their employers (Gaskin, 1998).

One common method for managing cyberloafing activities is the implementation of electronic use policies and control systems (Mirchandani, 2003, 2004; Straub and Welke, 1998). Once the internet use policies have established what actions are appropriate and acceptable to an organization, control systems are designed to deter abuse of company-provided e-mail and internet systems by discovering incidents and identifying the perpetrators. In a recent survey, Flynn (2005) found that over 80 percent of employers have implemented electronic use policies.

Unfortunately, despite the frequent use of control systems to combat cyberloafing, the literature only offers anecdotal advice for constructing these systems, the advice is not based on theory, and its effectiveness has not been empirically tested (Henle *et al.*, 2009). Furthermore, some prior work suggests that control systems by themselves may not have an inherent ability to either ethically demotivate (Cialdini, 1998) or rationally deter (Tenbrunsel and Messick, 1999) inappropriate behavior in organizations. Instead, some authors have suggested that control systems are influenced by determining factors (Alder *et al.*, 2008) and within broader mechanisms that ultimately decrease inappropriate behavior. In this regard, Blanchard and Henle (2008, p. 1080) noted that for efficient cyberloafing management to take place, "monitoring activities need to be followed up with disciplinary actions." Although at one time investigated ad nauseam, disciplinary actions are currently a subject of limited study (Young and Case, 2004; Mahatanankoon, 2006). Furthermore, recent studies suggest that it is not clear whether the management literature in traditional contexts is directly applicable to the specific settings (Maruping and Agarwal, 2004) in which cyberloafing takes place (e.g. more perceived anonymity, fewer social sanctions, and less recognition). Thus, it is imperative for scholars and practitioners to examine how and when control systems can deter cyberloafing, so that companies and organizations can harness their potential benefits.

The present study intends to shed light on this gap. From a strict deterrence approach, this paper suggests that control systems are ineffective in deterring cyberloafing unless cyber loafers view them as followed up by punitive consequences. In other words, standing alone, control systems are likely to be perceived as a sort of "ineffectual dog that may bark a lot, but ultimately does not bite." Given the easy visibility of cyberloafing activities, this paper first proposes control systems that include general perceptions of organizational control (hereafter, monitoring) as well as those related to supervisor physical proximity. The paper will then examine whether these control systems alone (supervisor physical proximity and monitoring) deter employees from engaging in cyberloafing. We expect that only under fear of formal punishment (hereafter, punishment), or "perceived certainty that the dog that really bites," can control systems "bring cyber loafers back on the right track." Finally, the paper will offer theoretical and practical implications derived from the results.

2. Theoretical background and hypothesis

Organizational and psychological research literatures offer two main strategies for controlling employee misconduct:

1. intrinsically oriented self-regulatory strategies; and
2. extrinsically oriented coercive strategies (from Lat. *coercĭo, -ōnis*: to contain, restraint, repression), where employees' behavior is enforced by external contingencies in their environment (Tyler and Blader, 2005).

The self-regulatory approach is linked to intrinsic motivational models of human behavior, in which employees decide not to engage in deviance based on their internal desires, preferences, and values (Kelman, 1958; Kelman and Hamilton, 1989; O'Reilly and Chatman, 1986). This approach in the workplace commonly uses fair procedures and respectful supervision, as well as allocating resources in a way that employees perceive as fair (see Conlon *et al.* (2005), for a review). Coercive strategies, on the other hand, are linked to extrinsic motivational models of employee behavior, in which employees act rationally by weighing the benefits and costs of a decision (Blair and Stout, 2001). While the boundaries of the impact of each strategy are difficult to establish in practice, coercive strategies influence employees' decisions to refuse to engage in deviance by means of deterrent contingencies, such as those that increase the perceived likelihood of being caught and punished.

All of the above strategies are present within the literature on cyberloafing. For example, Lim (2002) and Beugré (2006) found that designing a workplace perceived by employees as fair could constitute an effective self-regulatory strategy to manage cyberloafing. Sanctioning and monitoring systems, on the other hand, are common tools used to implement the cyberloafing-coercion strategy in the workplace (Liao *et al.*, 2010; Mirchandani, 2003, 2004; Straub and Nance, 1990; Straub and Welke, 1998; Zoghbi *et al.*, 2006). Finally, some studies have also made an effort to integrate these two approaches. These mixed strategies not only incorporate deterrent mechanisms in trying to influence cyber loafers through rationalizations, but also give, for instance, advance notice of electronic monitoring (Hovorka-Mead *et al.*, 2002; Stanton, 2000) and consistency in disciplinary procedures (Ball *et al.*, 1994; Youngblood *et al.*, 1992). In doing so, they also try the cyber loafers perceive these deterrent mechanisms as fair, trustworthy and legitimate (Henle *et al.*, 2009; Kankanhalli *et al.*, 2003; Kidwell and Bennett,1994; Lee and Lee, 2002; Lee *et al.*, 2004), so that they might be less intrinsically motivated to cyberloaf.

Do cyberloafing-control systems work? On a theoretical basis, monitoring that tracks internet and e-mail activity should be an important tool to discover incidents and identify the perpetrators. Straub and Nance (1990), in their classic study on computer abuse, found that normal system controls and purposeful investigations were able to discover up to 66 percent of the incidents. Moreover, Hsaio *et al.* (1979) and Kwok and Longley (1999) suggested that measures against computer misuse, such as physical security of facilities, cable security, and security software (e.g. password protection), are effective in misuse detection. However, results from recent studies are generally inconclusive in indicating whether control systems, irrespective of punishment, are able to deter the perpetrators of computer misuse activities. Interestingly, Zoghbi *et al.* (2006) found that monitoring decreases cyberloafing, and punishment actually increases it. However, many other studies have indicated that monitoring policies and systems are not effective in altering individuals' internet behavior (Galletta and Polak, 2003; Lee *et al.*, 2004). These researchers suggest that the ineffectiveness of monitoring could be related to how the monitoring has been implemented, its perceived usefulness, lack of punishment, issues related to privacy or employees' individual differences (Alder *et al.*, 2008).

Explanations based on the deterrence approach are consistent with the arguments mentioned above. By detecting incidents and identifying perpetrators, monitoring systems indeed help to elicit perceptions of the likelihood of being caught (probability of detection). However, they do not contribute to eliciting perceptions of the likelihood of being sanctioned (cost of detection). Rather, they appear to act as only one piece in the complex mechanisms that ultimately decrease cyberloafing activities:

H1. Monitoring has no main effects on cyberloafing.

The *raison d'être* of control systems is to play a detection role. A close look at the classic tools to deter users from computer abuse reveals that detection factors appear to act in a two-fold way (Kwok and Longley,1999; Straub and Nance, 1990). In addition to general perceptions of monitoring (e.g. deterrent certainty, password protection, cable security, or equipment maintenance), physical measures of control (e.g. physical security of facilities or physical entry controls) are also likely to be effective in managing cyberloafing (Pors, 2001). Supervisor physical proximity (hereafter, proximity) would refer to the extent to which employees perceive that their supervisor is physically close to them (Murphy *et al.*, 2003). The effective contribution of perceptions of proximity to workplace behavioral control finds support in classic literature (Bass, 1990; Milgram, 1974; Schrag, 1954; White and Lippitt, 1968). Overall, proximity increases the supervisor's opportunity to interact with employees (Bass, 1990); thus, proximity could make it easier for supervisors to determine whether the employee is slacking (George, 1992; Jones, 1984; Murphy *et al.*, 2003). Unfortunately, it is unlikely that single perceptions of proximity can increase the cyber loafers' sense of being controlled unless proximity is interpreted as a monitoring presence. Thus, proximity's success in communicating organizational alertness to cyber loafers might depend on having simultaneous perceptions of proximity and monitoring. However, in addition to a perceived certainty of being caught, as we argued above, deterrence is possible only to the extent that employees perceive a certainty of being sanctioned as well. Thus, we postulate the following:

H2. Proximity has no main effects on cyberloafing.

H3. Proximity and monitoring acting together have no interactive effects on cyberloafing.

Numerous empirical studies have suggested that the threat of punishment encourages people to act according to rational (rather than ethical) behavioral patterns (Tenbrunsel and Messick, 1999). Threats of punishment would lead employees to psychological reactance, that is, to believing they are expected to misbehave (Cialdini, 1998), which, in turn, would inhibit employees' intrinsic motivations to act ethically. Therefore, within a context in which cyber loafers are intimidated by threats of formal punishment, it is very unlikely that they will decide to "come back on the right track" only because they consider cyberloafing to be an unethical behavior, or due to their perceptions of the fairness of the control systems or the disciplinary process (Tenbrunsel and Messick, 1999). Instead, they make "business" decisions about whether to engage in cyberloafing which are highly influenced by the expected costs of engaging in it (expected cost = cost of detection × probably of detection).

Control systems and punishment acting separately are unable to increase the "expected cost" of engaging in cyberloafing, because, on the one hand, punishment only leads employees to evaluate the "cost of detection" if they are caught. On the other hand, control systems can only increase the "probability of detection." Thus, to deter cyber loafers from decisions to "go or continue on the wrong track," proximity, monitoring, and punishment should act together in an interactive way. We hence predict that the possible negative effects of control systems (proximity and monitoring) on cyberloafing will be conditioned or moderated by punishment (Figure 1). Only so, we could assert in metaphorical terms that control systems can no longer be perceived as a "barking dog that does not bite." Now "the dog really bites":

H4. Proximity and monitoring will only reduce cyberloafing if they interact with each other, and with punishment, on cyberloafing.

3. Method

Procedure and sample characteristics

Data were collected from 147 (19.4 percent) of the 758 administration and services personnel at a Spanish State University by means of a questionnaire posted on the intranet, which could be accessed by clicking on a link in the e-mail asking for collaboration. In recent years, the organization's internet usage policy to combat inappropriate use has been increasingly tough, especially toward employees and students. Under that policy, the organization uses software that monitors internet usage. Some individuals have been warned about cyberloafing, but the organization was not able to disclose actual numbers due to confidentiality.

The sample consisted of 50.7 percent males and 49.3 percent females and, while 47.4 percent were 40 years old or younger, 6.6 percent were 60 or older. 46.7 percent were civil servants, and the remainder were non-permanent staff. Since the university studied has outsourced the vast majority of services (e.g. internal mail, cleaning, repairs and maintenance, etc.), the sample comprises office employees whose main working tool

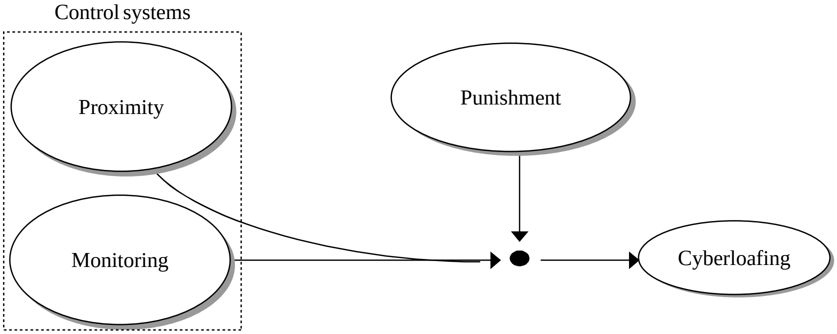

Figure 1.
Hypothesized model of punishment as moderator of the relationship between both proximity and monitoring, and cyberloafing

is the computer. All of them have internet access and individual e-mail, stable physical location at work, and direct supervision. In addition, the research project received prior official approval, IP addresses were unidentifiable, and the participants surveyed were so informed in order to avoid interference and reticence in responding. Eventually, there were 147 valid responses after five were rejected due to incorrect completion and seven due to incoherent information.

Measures

All items were scored on a seven-point scale ranging from (1) strongly disagree to (7) strongly agree – and for cyberloafing from (1) never to (7) constantly, and they are presented in Table II. The main diagonal of Table I shows the α coefficients. We plan to use structural equation modeling to ensure that the following variables are four separate constructs:

(1) *Proximity*. We used a three-item scale designed after a review of the literature related to the study of physical proximity in organizations (Kleck *et al.*, 1966; Monge and Kirste, 1980; Monge *et al.*, 1985), leadership proximity, and task visibility (George, 1992; Ronan *et al.*, 1973). Scores on two items were inverted before being entered in the analysis.

(2) *Monitoring*. The five-item scale used to measure this variable was constructed on the basis of a review of the literature on leadership as an instrument of goal achievement (Tucker, 1981) and organizational control (Friedman, 1977; Howell, 1988). The items were worded in such a way that the figure of the controller agent appeared as impersonal. Examples would be, "I may be accused at any moment" [. . .], and [. . .] "the proper use of my work tools may be checked" [. . .].

(3) *Punishment*. The six-item scale used to measure this variable was based on the stated levels of severity of disciplinary action established by Trahan and Steiner (1994). We selected six of the 12 levels studied by these authors, considering the real possibility of our respondents being punished in the case of theoretical deviant behavior in the workplace. We took into account the specific characteristics of the disciplinary procedure at the organization researched.

(4) *Cyberloafing*. We used a five-item scale adapted from the one proposed by Lim (2002), which included eight items referring to browsing activities and three to e-mailing activities. We selected four of the former, and one of the e-mail

Variables	M	SD	1	2	3	4	5	6
1. Gender	1.49	0.50	–					
2. Age	2.58	0.59	−0.003	–				
3. Proximity	2.78	1.29	−0.043	0.024	*0.656*			
4. Monitoring	3.64	1.32	−0.132	0.066		*0.734*		
5. Punishment	2.46	1.66	0.044	−0.065	0.298^{***}	0.401^{***}	*0.902*	
6. Cyberloafing	3.16	1.53	0.061	-0.212^{*}	−0.024	−0.086	0.216^{**}	*0.847*

Notes: Significance at: $^{*}p < 0.05$, $^{**}p < 0.01$, and $^{***}p < 0.001$ levels, respectively; the numbers in italics on the diagonal are α coefficient; gender: 1 – male, 2 – female; age: 1 – 23-30; 2 – 31-40; 3 – 41-50; 4 – 51-60; 5 – 61-70; 6 – 71-75

Table I.
Means, standard deviations, correlations and reliabilities

Table II. Variable items used in this study

Measure	
Supervisor physical proximity (proximity)	
X1. I feel that my supervisor moves around too closely to my personal workstation	0.82
X2. I cannot say that my supervisor appropriates my job privacy through physical proximity (*R*)	0.53
X3. My supervisor moves around so far from my workstation that I sometimes feel isolated from him (*R*)	0.53
Perceived organizational control (monitoring)	
Y4. I perceive that my co-worker and (or) client relationships are controlled by the university	0.74
Y5. I perceive pressure to achieve goals in my job	0.72
Y6. I perceive that the proper use of my work tools may be checked by my organization	0.71
Y7. I may be accused at any moment of not strictly fulfilling my job obligations	0.41
Fear of formal punishment (punishment)	
I recognize that I have sometimes complied with the rules of my job [. . .]	
Y8. For fear of a verbal caution from my boss	0.93
Y9. For fear of a warning/letter of reprimand from my boss	0.88
Y10. For fear that my bosses will watch and control me more closely	0.78
Y11. For fear that my organization will start disciplinary action with the intention of dismissing me	0.76
Cyberloafing	
I use internet at work to [. . .]	
Y12. Visit web sites and digital newspapers to seek personal information	0.79
Y13. Download software or files for personal or family use	0.78
Y14. Visit the web site of my bank to consult my current account	0.76
Y15. Read or send personal (non-professional) e-mails	0.65
Y16. Surf the net and so escape a little	0.65

Notes: $C_{\min} = 119.338$; df $= 98$; $p = 0.070$; $C_{\min}/\mathrm{df} = 1.218$; GFI $= 0.904$; CFI $= 0.977$; TLI $= 0.971$; NFI $= 0.885$; RMSEA $= 0.039$; (*R*), reverse scored items

activities, which combined Lim's "send" and 'read' e-mail. Lim's third item, "check" e-mail, was omitted, since we believe it overlaps with 'read' e-mail. The scale is expected to be one-dimensional.

(5) *Control variables*. Drawing on the literature, we considered that gender and age could co-vary with our dependent and independent variables (Zellars *et al.*, 2002; Aquino *et al.*, 2004).

4. Results

Confirmatory factor analysis (CFA) results are presented in Table II, whereas Table I shows the scale means, standard deviations, reliabilities and correlations (*r*) among all the variables. An inspection of the CFA results in Table II reveals that the variables under study are indeed distinct constructs: the χ^2 is not significant ($p = 0.07$) and – except for the normed fit index (NFI) – the goodness of fit (GFI), comparative fit (CFI), and Tucker-Lewis (TLI) indices are clearly above 0.90. In addition, the results from Table I suggest that our variables are significantly correlated in some of the expected directions. In effect, no variables under study seem to be negatively correlated with cyberloafing, whereas punishment's effects on cyberloafing ($r = 0.216$; $p < 0.01$) could be an indication of its moderating role.

We tested the hypotheses using multiple hierarchical regressions (Cohen and Cohen, 1983) with cyberloafing as the criterion variable (Table II). However, first the variables were centered to reduce multicollinearity (Aiken and West, 1991). In trying to offer the best figures, we included all possible combinations of interactions among the variables under study. As the columns in Table III confirm, we entered all the possible two and three-way interactions. In Table III, column 1 displays the results of the three-way interaction and, hence the key data supporting *H4*. The remaining columns in Table III contain data about the main effects on cyberloafing and those from the different combinations of two-way interactions. Thus, they are the key results supporting *H1-H3*.

We then performed the following: first, the control variables were entered in Step 1, followed by our variables (proximity, monitoring, and punishment) in Step 2. The two-way interactions were added in Step 3. Finally, the calculations end with the addition of the three-way interaction in Step 4 – column 1. Table III presents the results, which include the standardized β coefficients, the R^2 change at each step of the regressions, the significance of each model, as well as the adjusted R^2 in the final step. The statistical significance of the standardized β coefficients, and the change in R^2 once the interaction terms had been added, were appraised to test the hypothesized interaction effects.

As we pointed out above, single associations and two- and three-way interactions (Table III – Steps 2-4) were used to test the hypotheses. Table III – Step 2 supports *H1* and *H2*, since it shows that no variable is significantly negatively associated with cyberloafing. Instead, punishment is repeatedly related positively and significantly to cyberloafing. Table III – Step 3 adds support to *H3*, given that monitoring and proximity, acting together on cyberloafing, have no significant interactive effects. Moreover, this two-way interaction does not explain a significant amount of incremental variance, nor do the other two-way interactions. In contrast, an inspection of the three-way interaction (Table III – column 1; Step 4) reveals a negative and significant interactive effect of proximity and monitoring together, and with punishment, on cyberloafing ($B = -0.332$; $p < 0.01$). Moreover, this three-way interaction explains a significant amount of incremental variance ($\Delta R^2 = 0.047$; $p < 0.001$). Based on the above results, the only way proximity and/or monitoring (both separately and jointly) reduced cyberloafing was by interacting with punishment. This pattern supports *H4*.

The significant effect of the proximity, monitoring, and punishment interaction on cyberloafing is graphically shown in Figure 2, following the method recommended by Aiken and West (1991). Values of the variables were chosen 1 SD below and above the mean. Simple regression lines were generated by entering these values in the regression equation, and cyberloafing was regressed on punishment for different levels of proximity and monitoring. Figure 2 shows that punishment only decreases the level of cyberloafing in situations with high levels of both proximity and monitoring, while in the remaining situations punishment increases cyberloafing. Low levels of both proximity and monitoring appear to enhance this increase (the slope is steeper here).

5. Discussion

Stressing employees' rational behavior, this study supports the effectiveness of the deterrence mechanisms in preventing cyberloafing. However, control systems alone were not shown to be effective. Only by interacting together with punishment they are able to ultimately decrease cyberloafing. This significant contribution to the literature is

Table III. Regression models testing different interaction effects of proximity, monitoring and punishment, on cyberloafing

	Cyberloafing							
	All interactions		Only proximity × monitoring		Only proximity × punishment		Only monitoring × punishment	
Y	β	t	β	t	β	t	β	t
Step 1								
Gender	0.062	0.756	0.062	0.756	0.062	0.756	0.062	0.756
Age	−0.214	-2.615^{*}	−0.214	-2.615^{*}	−0.214	-2.615^{*}	−0.214	-2.615^{*}
R^2	$\mathit{0.050}^{*}$		$\mathit{0.050}^{*}$		$\mathit{0.050}^{*}$		$\mathit{0.050}^{*}$	
Step 2								
Proximity	−0.068	−0.806	−0.004	−0.042	−0.084	−0.995		
Monitoring	−0.169	−1.903	−0.063	−0.737			−0.176	−1.998
Punishment	0.289	3.208^{**}			0.225	2.668^{**}	0.272	3.110^{**}
ΔR^2	$\mathit{0.069}^{*}$		*0.004*		$\mathit{0.046}^{*}$		$\mathit{0.065}^{**}$	
Step 3								
Proximity × monitoring	0.113	1.208	0.120	1.461				
Proximity × punishment	−0.047	−0.475			0.016	0.185		
Monitoring × punishment	0.085	0.240					0.145	0.427
ΔR^2	*0.010*		*0.014*		*0.000*		*0.001*	
Step 4								
Proximity × monitoring × punishment	−0.332	-2.764^{**}						
ΔR^2	$\mathit{0.047}^{***}$							
Adjusted R^2	0.121		0.034		0.064		0.084	
F (5-9, 147)	3.202^{***}		2.026		2.956^{*}		3.644^{**}	

Notes: Significance at: $^{*}p < 0.05$, $^{**}p < 0.01$, and $^{***}p < 0.001$; $n = 147$

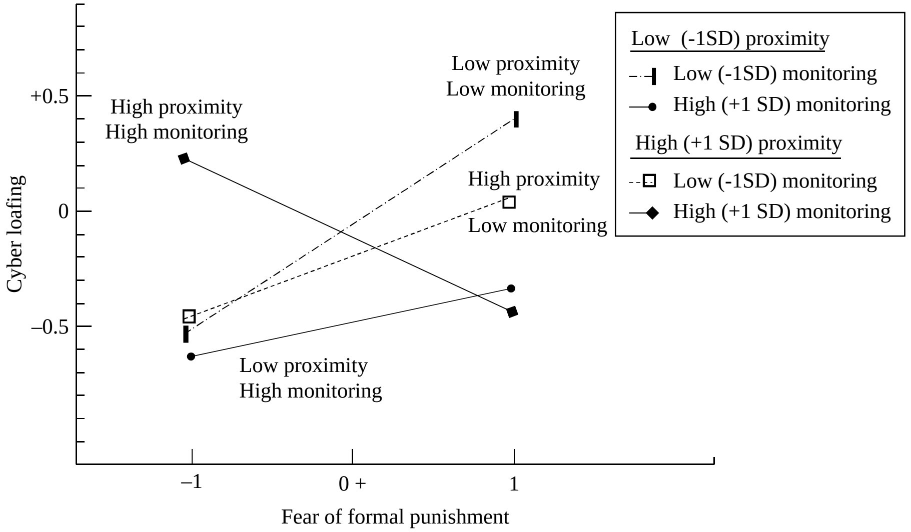

Figure 2.
Three-way interaction effects of proximity monitoring and punishment on cyberloafing

even greater if we consider the control system design used in this study, which included both monitoring and proximity. In that respect, Figure 2 shows that punishment only decreases cyberloafing in situations with high levels of both proximity and monitoring, while in situations with imbalanced and, especially, low levels of both proximity and monitoring, it appears to increase cyberloafing. Furthermore, together with punishment, low monitoring appears to fail to decrease cyberloafing, but high monitoring without high proximity is unable to deter cyberloafing either. As a result, only certain types and levels of control systems are effective in decreasing cyberloafing due to punishment. These findings are consistent with prior studies that state that only high (rather than low) levels of control are effective in promoting employee performance and ethical behavior (Spector, 1986; Hemmingsson and Lundberg, 1998).

However, punishment alone is not effective either. Given that punishment triggers cyberloafing when it acts alone (Table III – Step 2), and it becomes effective only when control systems are highly present (Figure 2), our results do not support its effectiveness in deterring cyberloafing by itself. This finding is also consistent with prior studies, such as Henle *et al.* (2009) and Zoghbi *et al.* (2006), which suggested that the employee perceptions of punishment could have no main effects on cyberloafing or even increase it. In this regard, Liao *et al.* (2010) did not support punishment severity and punishment certainty as being related to the employee intention to avoid internet misuse either. Furthermore, only if punishment is used as a threatening tool it appears to be helpful in deterring employees from cyberloafing, so that high levels of real impositions of sanctions appear to be quite irrelevant here and could even be an indicator of management failure. Thus, managers should ensure that their organization has well-designed cyberloafing-control strategies, not to sanction cyber loafers, but in order to warn employees that these measures are in place and will be followed up with punitive consequences. Nor should managers' aim be to try to inflict sanctions by surprise. The literature indeed distinguishes between contingent punishment, which is more likely to be perceived as just (Ball *et al.*, 1994), and erratic or arbitrary punishment.

Previous studies have shown that non-contingent punishment may produce undesirable effects, such as anxiety, depression, and lower levels of effort (Atwater *et al.*, 1998; deCharms and Hamblin, 1960; Cherrington *et al.*, 1971; Ward and Dugger, 2000). Our results support these findings by suggesting that punishment is only effective in deterring cyberloafing when it consists of contingent punishment, that is, punishment perceived to be applicable only if evidence of cyberloafing has been detected by control systems. Alone (i.e. perceived as indiscriminate or inconsistent), punishment triggered cyberloafing (Table III – Step 2), which suggests that "empty threats", without the direction that control systems provide to avoid them, lead employees to feel threatened but not controlled. They may not only perceive this situation as unjust (Ball *et al.*, 1994; Youngblood *et al.*, 1992), but also as unpunished. Impunity and injustice at the same time could lead them to perceive themselves as able to retaliate by engaging in cyberloafing, but without any risk. This idea is somewhat consistent with Zoghbi's (2006) prior study suggesting that unfair treatment by supervisors produces fear, which in turn leads employees to engage (or to take refuge?) in cyberloafing as their only escape.

In summary, what does this study suggest? First, it seems essential to check whether our supervisors really have negative attitudes toward cyberloafing activities. Only then can proximity (and probably monitoring as well) work, since it is properly interpreted by employees. Managers should then check to what extent offices are properly arranged for proximity, so that supervisors are able to move about near employees, the angles of orientation of employees' computer screens are easily visible to the supervisor, and the supervisor's desk is not hindered or isolated from proper visibility. Next, supervisors should check, and employees should perceive, that access control measures are in place and security mechanisms are operating. Finally, as the key point from our findings, information about penalties must be disseminated. However, rather than sanctioning them to mend their ways (behavioral change), these penalties should seek primarily to intimidate employees. Unfortunately, organizational managers sometimes have to initiate the disciplinary process and impose sanctions. In this case, it would be important and useful to distribute information about the sanctions handed out. Although communicating this information might be embarrassing, it could provide a key opportunity to shape employees' positive attitudes toward the control and disciplinary systems, which may increase their ability to deter future intentions to cyberloaf. This idea is consistent with some longitudinal studies that show that, although punishment can deter one from deviance, it may also have a weak or no effect on subsequent misconduct (see the meta-analysis in Pratt *et al.*, 2006). If sanctioning is conducted fairly (e.g. with consistency and advance warning), it should project a positive image to employees that will probably help to deter subsequent potential cyberloafing.

We should also indicate that the study has limitations. First, the study could suffer from mono-method/source bias. Second, although public university education in Spain is currently deregulated and, therefore, competes with the private universities, the state university that supplied the sample has certain job conditions (e.g. less threats of punishment) that are still inherent to workers in the public sector. Finally, the presence in the fear of punishment assessed of shades of other similar emotional constructs (e.g. exogenous anxiety or stress) cannot be ruled out.

This study also opens up several avenues for future research. Cyberloafing may not only influence employees' work and emotions as human-computer interaction phenomena (see Lim and Chen (2009) for a review), but it might also harm targets via the internet, that is, as behavior "delivered" via the internet (e.g. e-service, e-clients, e-mail system). Can they then be considered merely as abuse of internet resources? For the moment, if we are talking about behaviors that "exist" fundamentally as a consequence of the mechanisms of the internet, the ontology of these behaviors could also be seen as being linked to this fact. Otherwise, can we talk about the behaviors without simultaneously considering the medium that supports them? Based on the above, how would deterrent mechanisms against cyberloafing perform across virtual contexts? Could virtuality affect the way certainty and probability of detection of cyberloafing are perceived? Could virtual group membership influence or even suffocate the individual cyberloafing that occur when working alone?

In closing, the sensitivity of cyberloafing to the proposed trinomial of proximity, monitoring and punishment seems clearly supported. However, as we have repeatedly argued throughout this paper, this supported influence in preventing cyberloafing is not the result of a simple addition of each of the influences of these three variables. Rather, it is the result of a three-way interaction on cyberloafing. Thus, without "a barking dog that is perceived as able to bite," using control systems to "bring cyber loafers back from the wrong track" may be a useless practice.

References

Aiken, L.S. and West, S.G. (1991), *Multiple Regression: Testing and Interpreting Interactions*, Sage, Newbury Park, CA.

Alder, G.S., Schminke, M., Noel, T.W. and Kuenzi, M. (2008), "Employee reactions to internet monitoring: the moderating role of ethical orientation", *Journal of Business Ethics*, Vol. 80 No. 3, pp. 481-98.

Aquino, K., Galperin, B.L. and Bennett, R. (2004), "Social status and aggressiveness as moderators of the relationship between interactional justice and workplace deviance", *Journal of Applied Psychology*, Vol. 34 No. 5, pp. 1001-29.

Atwater, L.E., Dionne, S.D., Camobreco, J.F., Avolio, B.J. and Lau, A. (1998), "Individual attributes and leadership style: predicting the use of punishment and its effects", *Journal of Organizational Behavior*, Vol. 19 No. 6, pp. 559-76.

Ball, G.A., Trevino, L.K. and Sims, H.P. (1994), "Just and unjust punishment: influences on subordinate performance and citizenship", *Academy of Management Journal*, Vol. 37 No. 2, pp. 299-322.

Bass, B. (1990), *Bass and Stogdill's Handbook of Leadership: Theory, Research, and Managerial Applications*, The Free Press, New York, NY.

Beugré, C.D. (2006), "Understanding dysfunctional cyberbehavior: the role of organizational justice", in Anandarajan, M., Teo, T. and Simmers, C. (Eds), *The Internet and Workplace Transformation*, M.E. Sharpe, Armonk, NY, pp. 223-39.

Blair, M. and Stout, L. (2001), "Trust, trustworthiness, and the behavioral foundations of corporate law", *University of Pennsylvania Law Review*, Vol. 149 No. 6, pp. 1735-810.

Blanchard, A.L. and Henle, C.A. (2008), "Correlates of different forms of cyberloafing: the role of norms and external locus of control", *Computers in Human Behavior*, Vol. 24 No. 3, pp. 1067-84.

Cherrington, D., Reitz, H. and Scott, W. (1971), "Effects of contingent and noncontingent reward on the relationship between satisfaction and task performance", *Journal of Applied Psychology*, Vol. 55 No. 6, pp. 531-6.

Cialdini, R.B. (1998), *Influence: Science and Practice*, Harper Collins, New York. NY.

Cohen, J. and Cohen, P. (1983), *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Erlbaum, Hillsdale, NJ.

Conlon, D.E., Meyer, C.J. and Nowakowski, J.M. (2005), "How does organizational justice affect performance, withdrawal, and counterproductive behaviour?", in Greenberg, J. and Colquitt, J.A. (Eds), *Handbook of Organizational Justice*, Lawrence Erlbaum, Mahwah, NJ, pp. 301-27.

deCharms, R. and Hamblin, R.L. (1960), *Structural Factors and Individual Needs in Group Behavior*, Washington University, St Louis, MO.

Flynn, N. (2005), *2005 Electronic Monitoring & Surveillance Survey*, American Management Association, New York, NY.

Friedman, A. (1977), "Responsible autonomy versus direct control over the labour process", *Capital & Class*, Vol. 1, pp. 43-57.

Galletta, D.F. and Polak, P. (2003), "An empirical investigation of antecedents of internet abuse in the workplace", *Proceedings of the 2nd Annual Workshop on HCI Research in MIS, Seattle, WA*, pp. 12-13.

Gaskin, J.E. (1998), "Internet acceptable usage policies", *Information Systems Management*, Vol. 15 No. 2, pp. 20-5.

George, J.M. (1992), "Extrinsic and intrinsic origins of perceived social loafing in organizations", *Academy of Management Journal*, Vol. 35 No. 1, pp. 191-202.

Greenfield, D.N. and Davis, R.A. (2002), "Lost in cyberspace: the web @ work", *Cyberpsychology & Behavior*, Vol. 5 No. 4, pp. 347-53.

Hemmingsson, T. and Lundberg, I. (1998), "Work control, work demands, and work social support in relation to alcoholism among young men", *Alcoholism: Clinical and Experimental Research*, Vol. 22 No. 4, pp. 921-7.

Henle, C.A., Kohut, G. and Booth, R. (2009), "Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: an empirical test of justice theory", *Computers in Human Behavior*, Vol. 25 No. 4, pp. 902-10.

Hovorka-Mead, A.D., Ross, W.H., Whipple, T. and Renchin, M.B. (2002), "Watching the detectives: seasonal student employee reactions to electronic monitoring with and without advance notification", *Personnel Psychology*, Vol. 55 No. 2, pp. 329-62.

Howell, J.M. (1988), "Two faces of charisma: socialized and personalized leadership in organizations", in Conger, J. and Kanungo, R. (Eds), *Charismatic Leadership: The Illusive Factor in Organizational Effectiveness*, Jossey-Bass, San Francisco, CA.

Hsaio, K., Kerr, D. and Madnick, S. (1979), *Computer Security*, Academic Press, New York, NY.

Jones, G.R. (1984), "Task visibility, free riding, and shirking: explaining the effect of structure and technology on employee behavior", *Academy of Management Review*, Vol. 9, pp. 684-95.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-54.

Kelman, H.C. (1958), "Compliance, identification, and internalisation", *Journal of Conflict Resolution*, Vol. 2 No. 1, pp. 51-60.

Kelman, H.C. and Hamilton, V.L. (1989), *Crimes of Obedience*, Yale University Press, New Haven, CT.

Kidwell, R.E. and Bennett, N. (1994), "Employee reactions to electronic control systems: the role of procedural fairness", *Group and Organization Management*, Vol. 19 No. 2, pp. 203-18.

Kleck, B., Ono, H. and Hastorf, A.H. (1966), "The effects of physical space upon face-to-face interaction", *Human Relations*, Vol. 19, pp. 425-36.

Kwok, L.F. and Longley, D. (1999), "Information security management and modelling", *Information Management & Computer Security*, Vol. 7 No. 1, pp. 30-9.

Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management & Computer Security*, Vol. 10 No. 2, pp. 57-63.

Lee, S.M., Lee, S.G. and Yoo, S. (2004), "An integrative model of computer abuse based on social control and general deterrence theories", *Information & Management*, Vol. 41 No. 6, pp. 707-18.

Levoie, J.A.A. and Pychyl, T.A. (2001), "Cyberslacking and the procrastination superhighway: a web-based survey of online procrastination, attitudes, and emotion", *Social Science Computer Review*, Vol. 19 No. 4, pp. 431-44.

Liao, Q., Luo, X., Gurung, A. and Li, L. (2010), "Workplace management and employee misuse: does punishment matter?", *Journal of Computer Information Systems*, Vol. 50 No. 2, pp. 49-59.

Lim, V.K.G. (2002), "The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice", *Journal of Organizational Behavior*, Vol. 23 No. 5, pp. 675-94.

Lim, V.K.G. and Chen, D.J.Q. (2009), "Cyberloafing at the workplace: gain or drain on work?", *Behaviour & Information Technology*, Vol. 28 No. 5, pp. 421-31.

Mahatanankoon, P. (2006), "Internet abuse in the workplace: extension of workplace deviance model", in Anandarajan, M., Teo, T. and Simmers, C. (Eds), *The Internet and Workplace Transformation*, M.E. Sharpe, Armonk, NY, pp. 15-27.

Malachowski, D. (2005), "Wasted time at work costing companies billions", available at: www.sfgate.com/bin/.cgi?f=///2005///.TMP (accessed October 30, 2006).

Maruping, L.M. and Agarwal, R. (2004), "Managing team interpersonal processes through technology: a task-technology fit perspective", *Journal of Applied Psychology*, Vol. 89 No. 6, pp. 975-90.

Milgram, S. (1974), *Obedience to Authority: An Experimental View*, Harper & Row, New York, NY.

Mills, J.E., Hu, B., Beldona, S. and Clay, J. (2001), "Cyberslacking! A liability issue for wired workplaces", *Cornell Hotel & Restaurant Administration Quarterly*, Vol. 42 No. 5, pp. 34-47.

Mirchandani, D.A. (2003), "Reducing internet abuse in the workplace", *SAM Advanced Management Journal*, Vol. 68 No. 1, pp. 22-55.

Mirchandani, D.A. (2004), "A deterrence theory perspective on personal web usage", in Simmers, C.A. (Ed.), *Personal Web Usage in Workplace: A Guide to Effective Human Resources Management*, Information Science, Hershey, PA, pp. 111-24.

Monge, P.R. and Kirste, K.K. (1980), "Measuring proximity in human organization", *Social Psychology Quarterly*, Vol. 43 No. 1, pp. 110-15.

Monge, P.R., Rothman, L.W., Eisenberg, E.M., Miller, K.I. and Kirste, K.K. (1985), "The dynamics of organizational proximity", *Management Science*, Vol. 31 No. 9, pp. 1129-41.

Murphy, S.M., Wayne, S.J., Liden, R.C. and Erdogan, B. (2003), "Understanding social loafing: the role of justice perceptions and exchange relationships", *Human Relations*, Vol. 56 No. 1, pp. 61-84.

O'Reilly, C.A. and Chatman, J.A. (1986), "Organizational commitment and psychological attachment", *Journal of Applied Psychology*, Vol. 71 No. 3, pp. 492-9.

Pors, N.O. (2001), "Misbehaviour in the public library: internet use, filters and difficult people", *New Library World*, Vol. 102 No. 9, pp. 309-13.

Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E. and Madensen, T.D. (2006), *The Empirical Status of Deterrence Theory*, Transaction, New Brunswick, NJ.

Ronan, W.W., Latham, G.P. and Kinne, S.B. (1973), "Effects of goal setting and supervision of worker behavior in an industrial situation", *Journal of Applied Psychology*, Vol. 58 No. 3, pp. 302-7.

Schrag, C. (1954), "Leadership among prison inmates", *American Sociological Review*, Vol. 19, pp. 37-42.

Sipior, J.C. and Ward, B.T. (2002), "A strategic response to the broad spectrum of internet abuse", *Information Systems Management*, Vol. 19 No. 4, pp. 71-9.

Spector, P. (1986), "Perceived control by employees: a meta-analysis of studies concerning autonomy and participation at work", *Human Relations*, Vol. 39 No. 11, pp. 1005-16.

Stanton, J.M. (2000), "Traditional and electronic monitoring from an organizational justice perspective", *Journal of Business and Psychology*, Vol. 15 No. 1, pp. 129-47.

Straub, D.W. and Nance, W.D. (1990), "Discovering and disciplining computer abuse in organizations: a field study", *MIS Quarterly*, Vol. 14 No. 1, pp. 45-60.

Straub, D.W. and Welke, R. (1998), "Coping with systems risk: security planning models for management decision-making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-69.

Tenbrunsel, A.E. and Messick, D.M. (1999), "Sanctioning systems, decision frames, and cooperation", *Administrative Science Quarterly*, Vol. 44 No. 4, pp. 684-707.

Trahan, W.A. and Steiner, D.D. (1994), "Factors affecting supervisors' use of disciplinary actions following poor performance", *Journal of Organizational Behavior*, Vol. 15, pp. 129-39.

Tucker, R.C. (1981), *Politics as Leadership*, University of Missouri Press, Columbia, MO.

Tyler, T.R. and Blader, S.L. (2005), "Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings", *Academy of Management Journal*, Vol. 48 No. 6, pp. 1143-58.

Ward, C. and Dugger, J.C. (2000), "The impact of quality training on stress, anxiety and fear in the workplace", *Journal of School of Engineering Technology*, Vol. 16 No. 4, pp. 2-6.

White, R. and Lippitt, R. (1968), "Leader behavior and member reaction in three social climates", *Group Dynamics: Research and Theory*, Harper & Bros, New York, NY.

Young, K.S. and Case, C.J. (2004), "Internet abuse in the workplace: new trends in risk management", *CyberPsychology & Behavior*, Vol. 7 No. 1, pp. 105-11.

Youngblood, S.A., Trevino, L.K. and Favia, M. (1992), "Reactions to unjust discharge and third party dispute resolution: a justice framework", *Employee Responsibilities and Rights Journal*, Vol. 5 No. 4, pp. 283-307.

Zellars, K.L., Tepper, B.J. and Duffy, M.K. (2002), "Abusive supervision and subordinates' organizational citizenship behavior", *Journal of Applied Psychology*, Vol. 87 No. 6, pp. 1068-76.

Zoghbi, P. (2006), "Fear in organizations: does intimidation by formal punishment mediate the relationship between interactional justice and workplace internet deviance?", *Journal of Managerial Psychology*, Vol. 21 No. 6, pp. 580-92.

Zoghbi, P., Verano-Tacoronte, D. and Ting-Ding, J.M. (2006), "Do current anti-cyberloafing disciplinary practices have a replica in research findings? A study of the effects of coercive strategies on workplace internet misuse", *Internet Research*, Vol. 16 No. 4, pp. 450-67.

About the authors
Pablo Zoghbi-Manrique-de-Lara finished his PhD in Business Administration at Las Palmas de Gran Canaria University, Spain and is an Associate Professor in human resource (HR) management and organizational behavior of the Department of Economics and Management at same university. He spent six years in industry and finance, training, and HR management positions (mainly with El Corte Ingles and Ionics) prior to his return to academia. His primary research interests include issues surrounding the causes and consequences of deviant and citizenship behaviors in organizations. Pablo Zoghbi-Manrique-de-Lara is the corresponding author and can be contacted at: pzoghbi@dede.ulpgc.es

Arístides Olivares-Mesa finished his PhD in Business Administration at Las Palmas de Gran Canaria University, Spain, and is an Associate Professor in statistics and quantitative methods of the Department of Economics and Management at same university. His primary research interests include issues surrounding the area of global management and family business.