Information & Management 52 (2015) 170–182

Contents lists available at ScienceDirect

Information & Management

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

To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure

Jeremy Glassman, Marilyn Prosch, Benjamin B.M. Shao *

Department of Information Systems, W.P. Carey School of Business, Arizona State University, Tempe, AZ 85287-4606, USA

ARTICLE INFO

Article history:
Received 14 February 2014
Received in revised form 28 May 2014
Accepted 2 August 2014
Available online 12 August 2014

Keywords:
Cyberloafing
Internet filtering and monitoring
Agency theory
Operant conditioning
Procedural justice
Social norms

ABSTRACT

The goal of this study is to explore and analyze the effectiveness of a possible countermeasure to the so-called "cyberloafing" problem involving a technical solution of Internet filtering and monitoring. Through a multi-theoretical lens, we utilize operant conditioning and individuals' psychological morals of procedural justice and social norms to study the effectiveness of this countermeasure in addressing the associated agency problem and in promoting compliance with an organization's Internet usage policies. We find that in addition to the blocking module, confirmation and quota modules of an Internet filtering and monitoring system can prevent shirking and promote better compliance through employee empowerment and attention resource replenishment.

1. Introduction

Computers were initially created and used for primarily work-related functions. However, with the advent of the World Wide Web and ubiquitous computing, computers are also being used to engage in hobbies and to facilitate social connections. The use of web-enabled computing devices for both personal and business use has dramatically grown in recent years. Since computers and Internet access play an increasingly important role in the personal and professional lives of knowledge workers, the overlap between these two aspects has posed a serious issue for management across organizations [19].

In essence, the ubiquity of information technology (IT) and diffusion of the Internet have led to a prevalent mixture of personal and business Internet usage at work [4]. While users can access the Internet to complete their tasks more effectively, access to the Internet also increases the chance that they become distracted at work by engaging in activities such as shopping online, visiting news sites, emailing family and friends, or sharing pictures on social networks. This new type of loafing on the job has been coined as *cyberloafing* [25,26].

Muhl [31] found that in many organizations, management and employees have an implicit understanding that a certain amount of personal Internet usage is allowed at work. However, with the multitude of addicting Internet services such as social networks, games, and the ever-quickening news cycle [41], increasingly more employers are concerned that this "allowance" can be abused. Internet abuse by employees may affect organizations in several ways. For example, companies have to increase their IT expenditures, combat the exposure of their networks to potential threats, and monitor employee productivity more closely [34]. To reduce their exposure to these risks, organizations have adopted and implemented various control mechanisms, such as Internet usage policies [17] and software systems designed to block access to certain websites [38].

In a survey regarding compliance and enforcement of Internet usage policies [17], onerous web filtering rules and severe sanctions for non-compliance were found to have negative effects that are contrary to policymakers' intentions. Henle et al. [17] utilized personal norms to measure the likelihood of an employee to comply with Internet usage policies. They found that when facing increased severity of sanctions for non-compliance with Internet usage policies, employees with high personal norms were less likely to comply with the policies, while those with low personal norms were more likely to comply. Their finding suggests that effective solutions to cyberloafing need to be non-intrusive for employees who are more likely to comply with Internet usage policies but more direct for employees who are less likely to comply [28]. In addition, researchers in a cross-cultural study found that perceptions about the utilization and benefits of IT may affect employees' their usage of such technology [3].

* Corresponding author. Tel.: +1 480 727 6790; fax: +1 480 727 0881.
E-mail address: benjamin.shao@asu.edu (Benjamin B.M. Shao).

http://dx.doi.org/10.1016/j.im.2014.08.001
0378-7206/

The possibility for Internet abuse reflects an agency problem where employees (agents) and an employer (principal) have incongruent goals. In this context, information asymmetry between employees and the employer exists because the employer is unaware of how employees utilize the Internet resources of the organization [20]. As with most agency problems, monitoring is a possible solution, for example, through the use of an Internet filtering and monitoring software package in this case. The goal of this study is to investigate the effectiveness of a countermeasure to cyberloafing involving prolonged exposure to a conditioned stimulus that reinforces the notion that excessive non-work-related Internet use at work is unacceptable.

Sales of Internet filtering software indicate that its popularity is continually rising, as the combined revenue of leading companies in the Internet monitoring and filtering industry in 2012 was estimated to be $1.18 billion by Gartner Reports [32]. From their analysis, the market grew approximately 15% from 2011 to 2012, and they anticipate that the market will grow another 13% to 15% in 2013. The leaders in the Internet filtering and security market are Websense, Cisco, McAfee, and Bluecoat Systems, among others. Within the web filtering industry, various types of filtering systems are available. Currently available Internet filtering systems are all capable of blocking access to sites that are placed on a black list and/or allowing access to sites placed on a white list only. Some Internet filtering systems also monitor and record all employee access to the Internet and produce reports for management. Previous research provides evidence that Internet filtering systems do not sufficiently address the underlying issues associated with abusive Internet access and that such systems also engenders a sense of employee resentment about potential surveillance from the enforcement of Internet monitoring and filtering [38].

The rest of this paper is organized as follows: In the next section, we discuss different types of Internet usage filtering software that are available on the market and review the related theories that can be leveraged to study the agency problem of cyberloafing in the workplace. We then examine the individual filtering modules of an industry-leading Internet filtering system, state the goal of each module for hypothesis formulation, and link each module to the associated theories. The filtering system that we describe has been operating in a mid-sized diversified company, and we examine the monitoring data gathered by the organization for hypothesis testing to study the effectiveness of different Internet filtering modules. Finally, we discuss the results, their implications for practice, and future research directions before we conclude the paper.

2. Theoretical foundation

Prior research has examined several potential methods to mitigate inappropriate Internet usage, including the establishment of Internet usage policies, training, and monitoring. Researchers have found that periodic monitoring through software that tracks Internet usage reduces cyberloafing [17]. In a laboratory experiment, employees who were informed that their Internet usage would be electronically monitored were more task focused, meaning that they engaged in less cyberloafing than employees who were monitored with no knowledge of whether the monitoring system was actually implemented and functioning [38]. Hence, an electronic monitoring system alone is not a perfectly effective solution and has to be supplemented by other methods. One method to increase employees' awareness of an electronic monitoring system is through an established corporate policy to inform them of the presence of such a system documented by their signature [42]. Another method, which we examine in this study, is the use of a filtering mechanism to establish awareness of this monitoring policy and deter inappropriate use through the prohibition of cyberloafing activities.

The extant research on the phenomenon of abusive Internet practices at work focuses on short-term experiments to determine how users respond to deterrence systems. By contrast, the goal of this study is to investigate prolonged exposure to a conditioned stimulus that reinforces the notion that excessive non-work-related use of the Internet is unacceptable at work. In most existing web monitoring software, this conditioning process involves a managerial role that requires employees' supervisors to act on the information generated from a report and to inform users of their acceptable or unacceptable behavior. Existing related research has followed this approach where users were notified of their monitored actions if they had abused their Internet access [38]. In essence, a system that reminds users that the site they are visiting has questionable work value every time they access it provides real-time feedback to employees. Furthermore, such a system serves another purpose of deterrence by dissuading employees from abusing their Internet access. In the following subsections, we review relevant theories that pertain to the explanation of cyberloafing and its potential avoidance. The theories include agency theory, operant conditioning, procedural justice, and social norms.

2.1. Agency theory

The basis of agency theory is a relationship between a principal and an agent who acts on behalf of the principal [20]. Such relationships are formed when the owner of resources (principal) hires another party (agent) to perform work. The most recognizable form of an agency relationship is that of an employer (principal) and employees (agents). While both parties work toward the same goal, they may not always share the same interests. A key element of an agency problem is goal incongruence where the goal of the agent is inconsistent with that of the principal. When an agreement is made through mechanisms such as a contract, the lack of perfect information about the goals and productivity of the agent can lead to information asymmetry and can create a monitoring problem whereby the principal cannot easily observe the agent's actions or verify the information provided by the agent without exerting substantial effort or incurring considerable costs [12]. Common methods to address agency problems are engaging in intensive monitoring of agents and creating effective incentives to foster appropriate behavior.

Researchers in the IS field have used agency theory to explore various agency issues. For example, Dawson et al. [10] studied the relationship between consultants and clients, and they noted that a limitation of the application of agency theory is that the theory espouses monitoring as the primary method of combating the issues. In some cases, the intrinsic complexities of a situation with necessary specialized knowledge diminish the effectiveness of monitoring efforts. However, in our study, the technology being examined is able to automatically and effectively monitor employees in a workplace setting without involving substantial human intervention.

Inappropriate Internet usage is a prime example of a principal-agent relationship where the core issue can be viewed as an agency problem. In other words, cyberloafing illustrates an agency problem when an employee (agent) is cyberloafing and when he/she is doing so against the wishes of the employer (principal). Viewed from the perspective of agency theory, cyberloafing occurs because many organizations do not seek to specifically address this particular agency problem and, as a

consequence, do not verify whether employees have been using Internet resources appropriately.

2.2. Operant conditioning

Operant conditioning is the process of associating a particular behavior with a certain change in the subject's environment. This change can be a reinforcement involving a reward to strengthen a behavior or a punishment involving a penalty to discourage the behavior [39]. The difference between operant conditioning and other forms of behaviorism is that subjects can generate their own activities instead of only responding to external stimuli. According to this theory, behavior can be changed by creating consequences for the normal actions of a test subject. Reinforcement is a key element of operant conditioning. Positive reinforcers strengthen the desired response by instilling a sense of pleasure or contentment for the test subject. By contrast, negative reinforcers reprimand or cause displeasure for the test subject for engaging in inappropriate behaviors [35].

The use of a reinforcement schedule is an essential finding from the development of theory on operant conditioning. A schedule of reinforcement reflects the idea that an action will solicit only a temporary reinforcement feedback. In his experiments, Skinner [35] incrementally increased the variation of the schedules of reinforcement where a rat could press a lever to receive a food pellet. A continuous schedule of reinforcement is the control scenario where the rat receives a food pellet every time it presses the lever. With a fixed *ratio* schedule, a food pellet is given when the rat presses the lever for a constant, predetermined amount of time. A fixed ratio schedule is similar to a work environment where stipend payment is given for a pre-determined quantity of work performed. Another schedule of reinforcement is a fixed *interval* schedule, which uses a timing mechanism to enable or disable the food lever at a predetermined interval. With the fixed interval schedule of reinforcement, the number of pellets that can be dispensed is limited to one until the next interval, when one more pellet becomes available. The last type of schedule is a *variable* schedule of reinforcement. With a variable schedule, the reinforcer of a food pellet is given to the rat with constantly changing intervals and ratios. This variable schedule is found to be most effective for encouraging consistent actions in test subjects [35].

The idea of operant conditioning with a schedule of reinforcement can be applied to the context of Internet usage monitoring. The use of a passive monitoring system closely matches a variable schedule of reinforcement where a manager can generate reports based on a variable schedule and reprimand or dismiss an employee who has abused Internet access. In terms of operant conditioning, the way in which an employee browses the Internet is the behavior in focus in our study and the reprimand or dismissal of employees is the punishment.

2.3. Procedural justice

Cyberloafing stems from a failure of corporate governance policies and is a type of counterproductive work behavior. Counterproductive work behaviors (CWBs) include intentional behaviors of an organizational member that are viewed by an organization to be contrary to its legitimate interests [16]. The CWB of cyberloafing has been justified based on employees' attitudes toward job satisfaction and organizational commitment [2]. Many reasons have been given to explain why perceived organizational justice can affect CWBs. Increased perceptions of procedural injustice, for instance, can increase employees' unwillingness to comply with an organization's rules [7].

Previous research has shown that employee behavior is directly tied to the way in which governance policies are drafted and applied [15,44]. This phenomenon is directly linked to the social psychology theory of procedural justice. Procedural justice exists when procedures embody certain types of broadly accepted normative principles [27]. It has been shown that procedural justice is connected with cyberloafing and that organizational norms underlie workplace procedures [44]. When an employee is faced with seemingly unfair procedures, the Internet misuser may develop feelings of skepticism toward formal regulations and may perceive himself/herself as being involved in a conflict [6]. These negative perceptions of a normative conflict are found to mediate the relationship between procedural justice and cyberloafing [44].

Extant research has also shown that a relationship exists between procedural justice and employees' perceptions of conflicts at work [7]. Lind and Tyler [27] found that strong policies supporting a culture of procedural justice lead to fewer conflicts within organizations. Based on this finding, Kidwell and Martin [24] showed that conflicting rules and procedures, inflexible policies, and task difficulty increase employees' perceptions of unfairness. This feeling of unfairness, in turn, may trigger deviant behaviors that can harm an organization [24].

Procedural justice has also been used to explore individuals' attitudes toward perceived authority, as a feeling of fairness has been found to mediate attitudes toward authority [40]. In the case of cyberloafing prevention systems, transparent classification and reclassification of Internet sites would provide employees with a signal that they are being treated in a respectful and consistently fair manner. The utilization of procedural justice is also consistent with the practice of increasing employee empowerment [9]. Research has indicated that a satisfactory level of discretion is important for fostering employee empowerment in the workplace [23].

2.4. Social norms

Social norms are defined as "group-held beliefs about how members should behave in a given context, and these norms can be laws or informal guidelines that govern behavior in the society" [33]. People normally obey norms when they envision a particular outcome in mind. By abiding by norms, individuals aim to avoid the disapproval of others, which can range from receiving a raised eyebrow to being considered a social outcast of the "in" group. Social norms are distinguished from other social constructs. For example, social norms differ from legal norms because legal norms are enforced by individuals who are charged of upholding the norms (e.g., police officers), while social norms are enforced by one's peers, and the enforcement can sometimes be selective [13].

The workplace can be viewed as a venue for social norm-guided behavior [13]. Social norms in the workplace include the perception against living off the efforts of other people (i.e., shirking) and a corresponding pressure to earn one's income from one's own effort. Often, informal norms also exist among the co-workers of a firm who regulate the effort of other co-workers. These norms set upper and lower bounds of what is perceived to be an appropriate level of effort to prevent a feeling of "freeloading" off or, on the other end of the continuum, "outshining" fellow workers. These norms can also extend to the loyalty of co-workers, as it has been observed that workers within an organization sometimes have a code of honor that would forbid them for training new workers hired to do the same job for lower wages [1].

It is generally believed that workers favor leisure over effort and that they are therefore predisposed to shirking [36]. Shirking refers to the avoidance of work or other responsibilities in a work environment [22]. Cyberloafing constitutes a behavior in which an employee may engage as a form of shirking. A major responsibility of a firm's management is to provide incentives to assure worker performance, especially when monitoring information about

performance is costly [30]. In some cases, when incentivized, workers may even go against their own self-interests and provide extra value to their organization. Frey and Bohnet [14] conducted laboratory experiments and showed that people often act contrarily to their self-interest under the internal guidance of fairness and morality. This finding extends to the use of information systems and organizations' decision-making process for procuring effective IT resources to optimize work activities and reduce shirking.

Malhotra and Galletta [29] explored how social norms moderate users' system adoption and usage behavior. Their study provides a theoretical rationale for our inclusion of social norms as a potentially contributing factor to the acceptable use of Internet resources. Moreover, it has been shown that being allowed to take a break during work hours enables office workers to restore energy and their mental capacities [43]. Scheduled breaks as a norm, in turn, have been shown to improve task vigilance by replenishing employees' attention resources [18]. The core tenant of resource replenishment is that employees have a fixed amount of energy, and they focus their energy and resources to complete tasks. When they are working on a task, this bank of energy and focus is continually depleted. Research has indicated that by taking small breaks through the work day, this bank of energy and focus can be replenished; thus, the productivity of an employee who takes breaks is ultimately higher than that of an employee who does not [43]. In our context, studies have shown that engaging in cyberloafing activities during break time increases the rate at which the resource replenishment takes place [18].

3. Framework and hypothesis

Today, most organizations utilize some method to limit or monitor the Internet usage of their employees. The current industry standard is for Internet usage monitoring software to either reside on a stand-alone server or be incorporated into a service firewall. Various software packages can be configured with different modules to block, inhibit, or influence a user's access to the Internet.

At the root of cyberloafing is the existence of an agency conflict between the employees of an organization and its management. According to agency theory, the cause of the associated issue is the information asymmetry between the principal and the agents [20]. To combat this information asymmetry, monitoring is a proven solution, but monitoring alone with no subsequent consequences has been shown to be ineffective to prevent cyberloafing [38]. To augment a monitoring system in order to provide disincentives for inappropriate Internet use, we develop a framework that combines monitoring with the theory of operant conditioning. In our framework, operant conditioning is applied to modify an employee's behavior by utilizing methods derived from learning experiments [35]. In addition to operant conditioning, we utilize the theories of procedural justice and social norms to develop our research framework and study the agency problem of cyberloafing. Our Internet filtering framework is presented in Fig. 1.

Our Internet filtering framework relates to currently available Internet usage monitoring and classification software and mirrors the software's functions of classifying websites on the Internet into different categories. Our implementation of the software then groups these categories into four different response modules for the system to limit employees' access to the Internet. These response modules can be better explained and understood by comparing them to traffic lights and signs, as shown in Fig. 2. The first module consists of a white list for which the employee receives a "green light." This module measures appropriate use of Internet resources; thus, access to the white list is unrestricted at all times. The other extreme opposite from the white list is the black list. The black list can be compared to a "do not enter" sign, and employees are never allowed to visit these sites. In between these two extremes are potentially work-related sites (e.g., shopping) where employees are asked about the nature of their site visit for confirmation when the classification of the site itself is not able to determine the site's purpose. This confirmation module is similar to a "yield" sign. The final classification includes known leisure websites that have no direct work-related purpose but that help with positive morale by allowing some access to leisure websites. This category has a quota system that limits the amount of time that employees can spend visiting these sites and thus can be compared to a "yellow light."

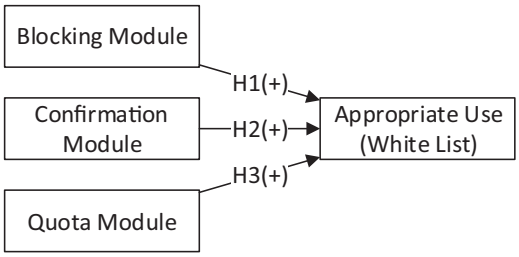

Fig. 1. Internet filtering framework.

We first articulate the theoretical justifications for the act of cyberloafing to develop the Internet filtering framework for counteracting cyberloafing. In our model, the variable of appropriate use can be tied to the construct of productive Internet usage. The blocking module can be linked to a measure of an employee's intention to shirk, which refers to the employee's avoidance of work or other responsibilities [22]. In regard to the quota module, research on attention resource replenishment has indicated that enjoyable breaks enable greater continued task vigilance than non-enjoyable breaks [8,18,43]. Extant research has also indicated that a positive correlation exists between employee empowerment and job satisfaction [37]. Our proposed framework includes a confirmation mechanism through which employees are empowered to bypass the filtering system when the site being visited is not on the black, white, or break list and hence when the system is unsure whether the intended Internet use is for work-related purposes. Such empowerment to decide for one's self can improve job satisfaction and productivity. In the following subsections, we discuss each module of the Internet filtering and monitoring system and present the associated hypotheses.

3.1. Appropriate use

The first component of the filtering system is an administrator-defined white list that enables employees to access all necessary

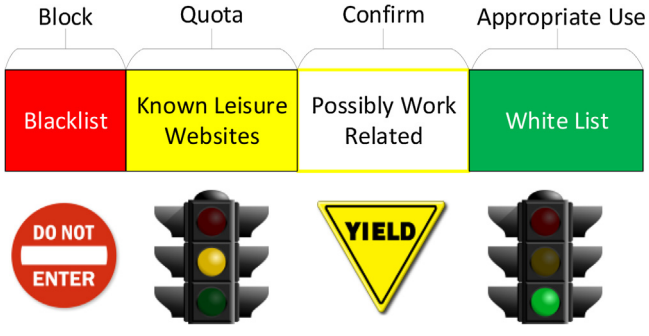

Fig. 2. Filtering category analogy.

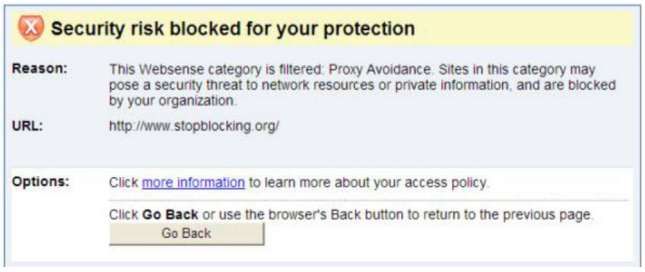

Fig. 3. Black list block prompt.

sites to complete their normal job function. The white list is a mechanism for employers to define what is considered appropriate use of the network resources at work. Therefore, access to the white list is used as the dependent variable for our analysis.

3.2. Blocking module

The second component is a black list that contains the websites that are considered to be counterproductive for work or potentially harmful and that are therefore blocked from access. When a user attempts to access these blacklisted sites and is blocked, the user is presented with a message explaining why access to the site has been blocked (as shown in Fig. 3), and he/she is asked to contact the administrator if the blocking is unwarranted. Consistent with operant conditioning and agency theory, when a user is presented with the blocking message, it conveys that the user is being monitored, and the user is presented with a link to the organization's policies. The policies explicitly state that employees will be held accountable for their actions. This blocking module along with the warning messages that it generates as stimuli is expected to enhance users' awareness of the monitoring policy and appropriate use of the Internet access. Therefore, we formulate our first hypothesis as follows:

H1: The usage of a blocking module is positively associated with the appropriate use of Internet resources.

3.3. Confirmation module

The next module is an active reminder mechanism to dissuade Internet abuse. When a user attempts to access a site that is not on either the white or the black list, the user receives a prompt message asking whether he/she intends to visit this possibly non-work-related site (see Fig. 4). Upon stating that the intended use of the target site is indeed work related, the employee will be allowed to visit the requested web page and be able to request additional pages from that site for a period of 5 minutes before being prompted again about the work-related nature of the site. The effect of the confirmation module on user behavior can be attributable to both agency theory and procedural justice theory. In essence, when the system renders employees an opportunity to confirm the content classification of the target website as correct and work related, the system fosters a sense of fairness and openness. This confirmation mechanism empowers employees, prevents a feeling of conflict with an organization's policies, and hence reduces employees' intention to cyberloaf [24]. A sense of fairness is engendered owing to the consistency of the organization's policies with the expectation that employees should work when they are paid to provide work [13,33]. We thus present our next hypothesis as follows:

H2: The usage of a confirmation module is positively associated with the appropriate use of Internet resources.

3.4. Quota module

The last module is an automated system to manage employee quotas for visits to leisure sites. Upon their first visit to a site that requires the use of their quota time, an employee will be presented with a page that grants 10 minutes of quota time for Internet usage, as shown in Fig. 5. After the 10 minutes expire, the employee will be directed to the same page again to request another 10 minutes of quota time if he or she wants to continue browsing the same non-work-related site. Employees' usage of quota time is recorded so that their managers can receive a report of quota time usage. If a user spends more than 90 minutes visiting questionable websites in one day, they will be directed to a page stating that they have exceeded their daily quota for web usage. The effect of this quota module on user behavior can be attributed to agency theory and social norms. Applying policies that limit users' non-work-related Internet use in a clear and transparent manner reinforces the social norms that work-related activities should be performed during work time and that cyberloafing is permissible during break time only. In addition, employees' attention resources can be replenished through the leisure website visits offered by the quota system, which can increase their productivity at work. Accordingly, we propose our last hypothesis as follows:

H3: The usage of a quota module is positively associated with the appropriate use of Internet resources.

3.5. Module relationships and decision flow

Our hypotheses are developed to examine whether the different filtering modules (i.e., blocking, confirmation, and quota) influence employees' appropriate use of Internet resources. To effectively assess the impacts of these modules on appropriate Internet use, the modules are organized into an enterprise Internet filtering system. The flowchart shown in Fig. 6 depicts the module

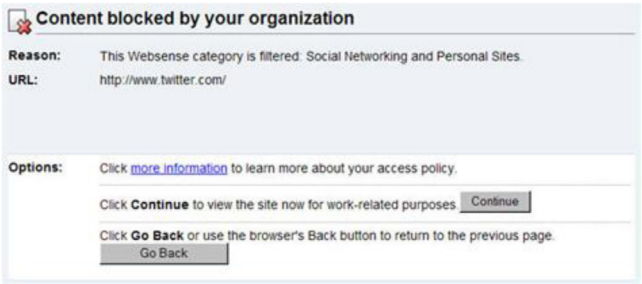

Fig. 4. Confirmation of work-related use prompt.

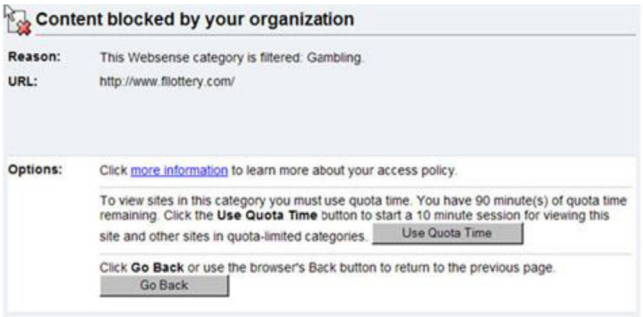

Fig. 5. Quota block prompt.

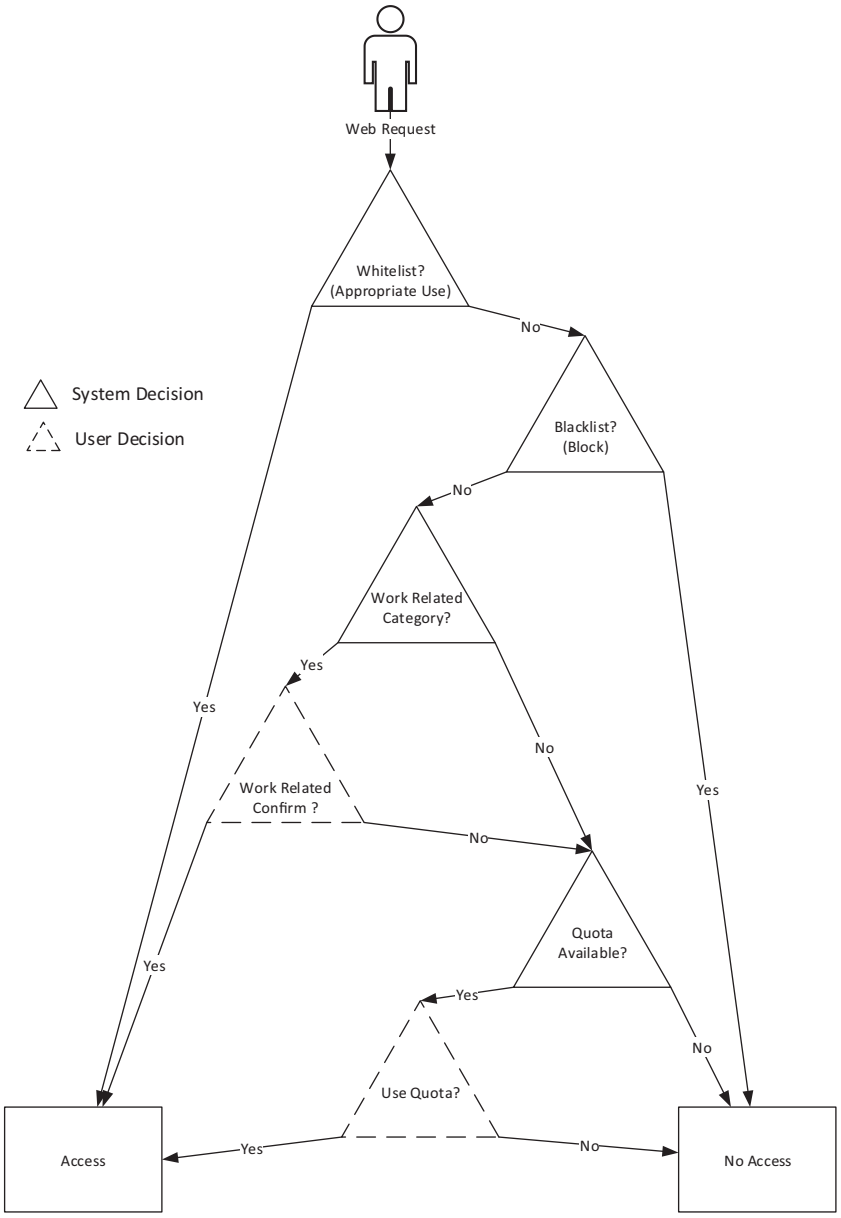

Fig. 6. Module relationships and decision flow.

relationships and the different decisions that are made in the process of Internet filtering and monitoring. The flowchart consists of two types of decisions that are made within the system: programmatic decisions and user decisions. Programmatic decisions (i.e., decisions predetermined by management and made by the system) are depicted as solid triangles in Fig. 6. These decisions are manifestation of an organization's Internet usage policies and can be considered a proxy for the principal in the principal–agent relationship in the context of cyberloafing. Regarding user decisions, users (agents) make two types of decisions, which are illustrated by dashed triangles in Fig. 6. At these prompts, the system asks users for information about the intended purpose of their website visit (i.e., business or personal), and if it is for personal use, the system then inquires whether they would like to use time within their quota allocation for the visit. These prompts can be viewed to give users discretion regarding their Internet usage in these types of situations.

4. Methodology and data

We collected actual usage data from a mid-sized, diversified company over a 6-month period. The organization that was used for our study consists of three main business units that are located in one western state of the United States:

- Three manufacturing plants that grow, process, and package fruits and vegetables;
- Fourteen retail agricultural chemical distributors; and
- One corporate office that includes an insurance agency, a private equity bank, and a transaction-processing department for accounts receivable and accounts payable.

The data set contains web filtering information for 275 employees over a period of 180 days from April 2011 to October 2011. The data include over 34 million records of requests for web content.

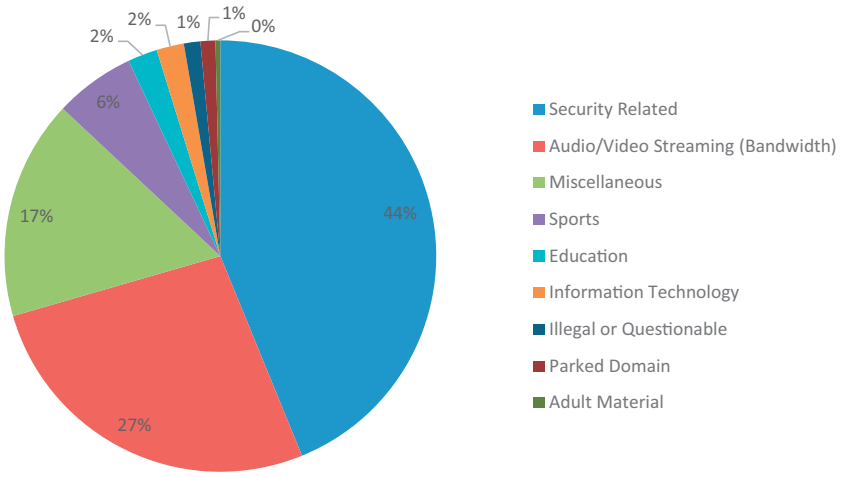

Fig. 7. Black list blocks by category.

The organization has a complex set of rules for filtering Internet usage. To enforce the organization's Internet usage policies, four separate components are enacted via a Websense Internet Filtering Suite. This Internet filtering product was purchased from Websense, Inc. (NASDAQ: WBSN), which is currently one of the market leaders in the web filtering industry [21]. Websense provides a complex hybrid filtering/monitoring system aiming to increase productivity among an organization's employees. The software package utilizes a web service and a proprietary database to dynamically categorize websites, and these categories are then assigned to the filtering modules that are used in this study.

In the organization, the white list includes all sites on the Internet that are deemed work related and all sites that are used for access to internal enterprise systems. Because the organization utilizes a service delivery method for their business applications via a web-based system, the number of each user's interactions with the websites on the white list is considered to be appropriate for the purpose of this study and is used as a proxy for the amount of network resources that employees access to complete their jobs. This white list is manually generated by the IT department of the organization and is updated only when changes in IT infrastructure or job functions occur. None of these events occurred during the period of our data collection. Thus, the white list remained fixed and unchanged throughout our study period.

The blocking module consists of a black list that contains all websites that are considered to be unproductive for work or potentially harmful and that are hence blocked from access. The most commonly blocked categories from this module are shown in Fig. 7. When users attempt to access such a site, they are presented with a message explaining why the site has been blocked, and they are instructed to contact the administrator if the blocking is unwarranted.

The next module is the confirmation module, where users are prompted to confirm whether their visit to a site is for work purposes. In this confirmation module, the category that is most commonly claimed to be work related is shopping, followed by travel. These two categories are also the most commonly blocked sites when employees admit that their visits to these sites are not actually work related (see Fig. 8).

The final module in the organization's implementation of the software is the quota module through which each user is granted 90 minutes of daily cyberloafing time comprising 50 minutes for lunch time and four 10 minute breaks. In the data, the most commonly visited category when quota time is activated is sports, followed by society and lifestyle (see Fig. 9). The figure shows the interactions that occur when a user attempts to access a category that is marked as quota and then chooses whether to use quota time to access the site. Fig. 9 also shows that users are more likely to use their quota time when prompted for sports websites, while users who are stopped from accessing society and lifestyle websites are less likely to use their quota time.

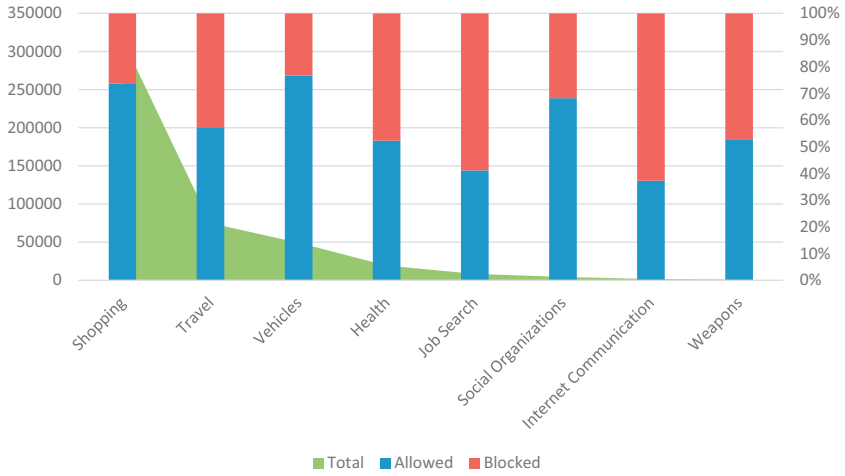

Fig. 8. Work-related prompts by category.

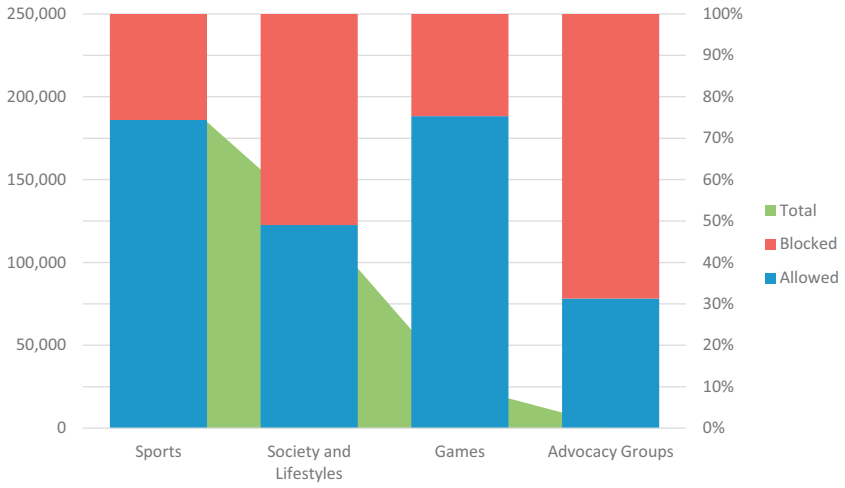

Fig. 9. Quota usage by category.

5. Analysis and results

5.1. Data description and analysis

Because of the organization's use of Websense's Internet filtering product, the data collection process was straightforward, as Websense stores all the data in a Microsoft SQL database. The original data set contained over 34 million user interaction records. The data set was summarized by user for each of the 5 independent variables and the dependent variable. Over the course of the 180-day period from April through October in 2011, 275 different user accounts were active and recorded by the organization.

The independent variables for the regression model of user interactions with the filtering system include Blocked by Category (Block), Blocked with Work-related Confirmation (Confirmation Block), Allowed with Work-related Confirmation (Confirmation Allow), Allowed via Quota (Quota Allow), and Blocked via Quota (Quota Block). The dependent variable is the number of recorded appropriate interactions with Internet sites based on the white list (Appropriate Use). For the organization under study, the Appropriate Use variable covers all Intranet sites. The organization utilizes web delivery for the majority of their enterprise applications; therefore, the Appropriate Use variable contains visits to work-related websites and the use of enterprise applications, making this variable a good proxy for work-related activities.

During the preliminary analysis of the data, significant variation was found within the number of appropriate interactions with websites among employees. After further analysis, some user accounts were found to fall outside what would be classified as a "normal user." After sorting the raw data by the number of interactions with sites on the white list, two major gaps in the data were uncovered. On the low end, a gap between 135 and 201 interactions was observed. After examining the details of the Internet traffic, all users below 200 interactions were believed to have been non-human user accounts that were used to update key enterprise systems; thus, these accounts were removed from the sample.

In addition to anomalies on the low end of the continuum of interactions, a similar irregularity occurred on the high end of the continuum. A gap existed between 287,444 and 314,534 interactions. After analyzing the group membership of these user accounts, these user accounts were found to belong to employees with an IT-related function or an executive whose traffic bypasses the filtering systems. Because of the differences between these users and users in the rest of the sample, all users above 287,444 interactions were also removed. The final data set thus contains 202 of the original 275 user accounts that were collected. OLS regression was then estimated based on the models in Eq. (1) and Eq. (2). The results of the response- and module-level analyses are presented in Table 1 and Table 2, respectively. Fig. 10 visually summarizes the outcomes.

$$\text{Appropriate Use} = \beta_0 + \beta_1\,\text{Block} + \beta_2\,\text{Confirmation Block} + \beta_3\,\text{Confirmation Allow} + \beta_4\,\text{Quota Block} + \beta_5\,\text{Quota Allow} + \epsilon \quad (1)$$

$$\text{Appropriate Use} = \beta_0 + \beta_1\,\text{Block} + \beta_2(\text{Confirmation Block} + \text{Confirmation Allow}) + \beta_3\,(\text{Quota Block} + \text{Quota Allow}) + \epsilon \quad (2)$$

Table 1
Regression results of response-level analysis.

	Standardized coefficients	p	Collinearity statistics		Descriptive statistics		
			Tolerance	VIF	Mean	Std. deviation	N
Appropriate Use					73,669.6	78,975.58	202
Block	0.244	0.00***	0.984	1.017	2541.77	7103.109	202
Confirmation Block	0.155	0.02*	0.786	1.273	607.45	1789.934	202
Confirmation Allow	0.318	0.00***	0.803	1.245	1356.01	3275.802	202
Quota Block	0.117	0.05*	0.957	1.045	460.56	1942.921	202
Quota Allow	0.13	0.03*	0.957	1.045	915.01	3475.296	202
			Model fit				
Adjusted R-squared		0.29	Std. error of the estimate			66,532.146	

* $= p < 0.05$.
** $= p < 0.01$.
*** $= p < 0.001$.

Table 2
Regression results of module-level analysis.

	Standardized coefficients	*p*	Collinearity statistics		Descriptive statistics		
			Tolerance	VIF	Mean	Std. deviation	*N*
Appropriate Use					73,670	78,975.58	202
Block	0.244	0.00**	0.986	1.014	2541.77	7103.109	202
Confirmation	0.411	0.00**	0.975	1.025	1963.46	4371.508	202
Quota	0.184	0.00**	0.967	1.034	1375.57	4240.889	202
			Model fit				
Adjusted *R*-squared		0.30	Std. error of the estimate			66,261.48442	

* = $p < 0.05$.
** = $p < 0.01$.
*** = $p < 0.001$.

As shown in Table 1, the results showed that the response-level model of Eq. (1) accounted for 29% of the variation in the appropriate use of network resources. We found that all coefficient estimates of the independent variables were significant at the .05 level or higher and that all three hypotheses were supported. The results of our analyses showed that the real-time Internet usage warnings implemented by the organization to combat cyberloafing were effective for enhancing the appropriate use of Internet resources.

In addition to the individual direct effects of the five independent variables on appropriate Internet use, we also estimated a module-level model (i.e., Eq. (2) and Table 2) for the effects of the three module groups shown in Fig. 10. This aggregate treatment more closely reflects our model proposed in Fig. 1. The results from the module-level model showed that the module with the greatest effect on appropriate Internet use was the confirmation module, followed by the blocking and quota modules. This finding provides support for the implementation of the three separate modules to enhance appropriate Internet use at work, as each module plays an active role in combating cyberloafing.

The results provide evidence showing that the use of Internet filtering and monitoring software for operant conditioning is an effective way of reducing cyberloafing. The results also lead us to conclude that the root of the cyberloafing problem in an organization is the existence of an agency conflict between the employees and the management of the organization. Nevertheless, the use of an IT-enabled countermeasure to reduce the information asymmetry associated with this agency problem is an effective solution to counteract cyberloafing, as supervisors can monitor employees by utilizing an active warning system to alert them about the presence of the monitoring system.

In addition, the results provide evidence that the confirmation module is most effective in increasing appropriate Internet use. In light of the theory of procedural justice, the results lead us to conclude that when a monitoring system renders employees an opportunity and hence the power to confirm that the content classification of a target website is correct and work related, the system fosters a sense of fairness and openness among employees. The confirmation mechanism therefore empowers employees, prevents feelings of conflict with the organization's policies, and reduces employees' intention to cyberloaf [24].

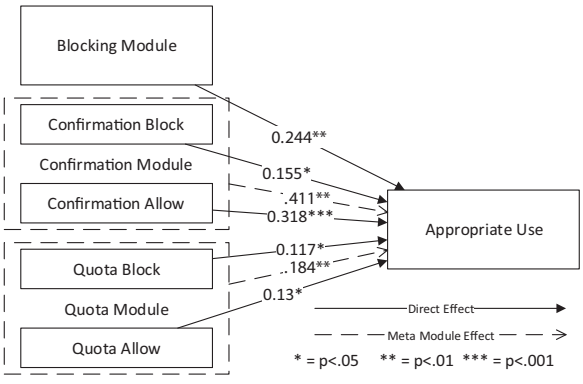

Fig. 10. Estimation outcomes.

As an explanation for the effectiveness of the confirmation module, procedural justice conveys a sense of fairness in the communication process that preemptively resolves potential disputes and that facilitates equitable resource allocation. In the communication process, procedural justice promotes perceptions of fairness regarding outcomes and reflects the degree to which an individual feels that outcome decisions have been fairly made. Fair procedures essentially help inform employees that they are valued by the organization. As a result, procedural justice is effective for communication and is important in the workplace. In other words, procedural justice derives from fair procedures, offers employees a voice in the decision process, offers them fair treatment, and allows them to have more input in the appraisal process. Employees will thus feel more appreciated, perform tasks to expected standards, and increase their job performance and productivity.

Our results show that the quota module is also effective for increasing appropriate Internet use. Based on the theory of social norms, the results lead us to conclude that when the system makes employees distinguish between work time and break time, they accept the expectation that they should work during work time and hence increase their appropriate use of Internet resources. Table 3 summarizes our major findings for each hypothesis in terms of their theoretical bases and outcomes.

5.2. Robustness analysis

During the data collection process, we requested data on other control variables from the organization. In an effort to make data on the control variables available for all system users, the organization exported information from two of their payroll databases. The data retrieved included a unique user ID, age, gender, and tenure with the organization. We then added an additional control variable indicating which of the two payroll databases the record was drawn since each payroll database was associated with a discrete business unit of the organization. When we attempted to match the payroll records with the previously collected data on users' usage of the web filtering system, inconsistencies in the user ID matching were encountered. After further investigation, these inconsistencies were determined to be caused by the fact that four payroll systems were used by the organization, but we were only granted access to data from two of them. This partial access to the data reduced our sample size for the control variables to 100 unique users. Moreover, while prior research on social norms has found that gender is a moderating variable of the effects of social norms [5], the gender information

Table 3
Major findings of analysis.

Hypothesis	Theory	Construct	Outcome	Finding
H1: The usage of a blocking module is positively associated with the appropriate use of Internet resources.	• Agency theory • Operant conditioning	Shirking as a form of agency problem	Supported	Agency theory describes the root problem for cyberloafing, while operant conditioning provides a method to mitigate the problem.
H2: The usage of a confirmation module is positively associated with the appropriate use of Internet resources.	• Agency theory • Operant conditioning • Procedural justice	Empowerment	Supported	Procedural justice contributes to a sense of fairness when an employee is asked to confirm the classification of a possibly work-related site.
H3: The usage of a quota module is positively associated with the appropriate use of Internet resources.	• Agency theory • Operant conditioning • Social norms	Resource replenishment	Supported	Social norms are reinforced when work and break times are delineated via the quota being granted.

for the organization was found to be unusable, as there were only two female employees among the 100 users. As a result, our control variables include age, tenure, and a Southwest (SW) dummy to represent one of the two payroll database sources.

Once the control variables were added to the regression models, the results for 100-user subsample (Table 4) were then compared with those for the original sample of 202 users (Table 2). We found that the main effects remained consistent in terms of the level of significance and directionality between the full sample and the subsample. When analyzing the regression results that included the controls (Table 4), we obtained a significant coefficient estimate for the dummy variable that represented which of the two payroll databases that a user belonged to. The significance of this location-related variable indicates that the associated population differs from the rest of the sample. To further investigate this difference, we conducted two more regressions to compare how the sample of users within the "SW" payroll database differs from the sample of users outside the "SW" payroll database.

The comparison of the two subsamples from the two payroll databases (see Tables 5 and 6) revealed differences in the main effects between these subsamples. The results showed that the blocking module did not significantly affect appropriate Internet use within the "SW" business unit and that the quota module did not significantly enhance appropriate Internet use outside the "SW" business unit. With respect to the other control variables, the only variable that was found to be significant was the user age for the "SW" business unit. Regarding this finding, we spoke with the management of the organization, and they indicated the management style of the "SW" business unit differs from that of the rest of the organization; thus, the different management styles may have led to the differences in our findings. This insight is useful for future studies to determine the source of these effects from users' point of view.

6. Discussion

The current study builds on previous research on cyberloafing [27,28] and utilizes data collected on employees' attitudes toward cyberloafing to provide insights for both researchers and practitioners. We analyze archival real world data to examine the effectiveness of the different Internet filtering modules of a leading commercial software system. Our framework is related to Lim and Teo's study [26] on how employees view cyberloafing activities, and our analysis of successful countermeasures using monitoring data is consistent with their findings. Researchers can leverage our findings to develop and test innovative measures to counteract cyberloafing, while practitioners can utilize the results to streamline their current Internet filtering systems and to identify the most effective countermeasures to address cyberloafing.

Our results showed that the confirmation module was most effective for filtering and monitoring Internet usage. Possible topics for future research based on this finding include the following:

(1) Why is the confirmation module the most effective? Our results suggest a need for further investigation to explore why empowerment through procedural justice increases effectiveness of the confirmation module. To address this question, a survey-based study on user perceptions and intentions would be required.
(2) Can user training, Internet usage policies, and other factors be a substitute for or complement of an Internet filtering and monitoring system? To cope with cyberloafing, other factors

Table 4
Regression results of module-level analysis with controls.

	Standardized coefficients		Collinearity statistics		Descriptive statistics		
	Beta	Sig.	Tolerance	VIF	Mean	Std. dev	*N*
Appropriate Use					76,994.56	80,681.707	100
Block	0.266	.002**	0.935	1.07	2555.25	5188.39	100
Confirmation	0.467	.000***	0.969	1.032	2715.09	5419.001	100
Quota	0.202	.019*	0.913	1.095	1919.11	5780.897	100
Age	0.031	0.77	0.597	1.674	42.28	12.31	100
Tenure	0.088	0.398	0.605	1.654	3482.67	3581.981	100
SW	−0.151	.068*	0.975	1.026	0.3	0.461	100
			Model fit				
Adjusted *R*-squared			0.3955	Std. error of the estimate			64,717.67

* $= p < 0.05$.
** $= p < 0.01$.
*** $= p < 0.001$.

Table 5
Results of module-level analysis with controls for the SW location.

	Standardized coefficients		Collinearity statistics		Descriptive statistics		
	Beta	Sig.	Tolerance	VIF	Mean	Std. dev	*N*
Appropriate Use					60,157.27	61,601.59	30
Block	−.166	.103	.870	1.149	3369.80	5334.03	30
Confirmation	.402	.000***	.880	1.137	2877.77	5997.09	30
Quota	.720	.000***	.861	1.162	1304.43	2853.58	30
Age	.313	.008**	.721	1.387	41.47	10.90	30
Tenure	−.067	.535	.728	1.373	3007.23	2767.98	30
			Model fit				
Adjusted *R*-squared			0.759	Std. error of the estimate			30,216.002

* = $p < 0.05$.
** = $p < 0.01$.
*** = $p < 0.001$.

may influence employee reactions to an Internet filtering and monitoring system. Examples include an organization's Internet usage policies, user training, culture, and managerial orientation, among others. These factors, however, cannot be verified with our data set. To answer this research question, a laboratory or field experiment would be required to collect user responses in order to assess the efficacy of user training, Internet usage policies, and other factors in a controlled environment.

(3) Do users abuse the confirmation module? While the confirmation module relies on a pre-specified list of categories, as listed in Fig. 8, to inquire whether the website to be visited is work related, there is no procedure to automatically verify and evaluate users' responses. Hence, users may abuse the confirmation module. However, we noticed that in the past, employees had been reprimanded by the organization for inappropriate web usage through the confirmation module. As such, we believe abuse of the confirmation module was not common among users during our study period. Nevertheless, it would be interesting to study whether users abuse the confirmation module if they are not reprimanded and, if so, to what extent.

After investigating the way in which users interact with Internet filtering systems, another interesting follow-up question concerns whether employees are simply limited by their interactions with the Internet filter or whether the Internet filter actually alters their behavior permanently. One way to test this conjecture in future research is to determine whether the employees' conditioned behavior returns to the previous norm, called *extinction*, once employees are no longer blocked by the system. Extinction is the extent of the decrease in the reinforced behavior once the frequency of the reinforcer is reduced or once the reinforcer is removed altogether [11]. Understanding and operationalizing this construct will help identify the underlying cause of the reduction in cyberloafing. In this study, we have taken the first step to show that an effect exists, but we cannot determine whether the nature of relationships between the different stimuli of the system is permanent or temporary. More research on this topic is thus warranted. Moreover, future research could examine whether filtering system warnings need to appear 100% of the time or whether intermittent (random) warnings are just as effective.

The process of asking users whether a visited site is work related and forcing them to utilize their quota time prevents the extinction of the conditioned behavior by promoting the notion that employees' actions are being constantly monitored by a sophisticated Internet filtering system. To study extinction in this setting, future research could measure how long employees' behavior remains changed since their last interaction with the system until their behavior returns to the previous baseline level. Prior research has shown that the realization of a system monitoring employees' actions is powerful enough to alter their behaviors for a short duration [38].

By studying the rate of reoccurrence of inappropriate behaviors based on the different filtering modules of the system, the learning process involved in using the system can be analyzed. One unanswered question concerns whether employees have actually learned that their behavior was unacceptable. Thus, future research could study whether employees adjusted their behavior permanently or whether they just changed their behavior temporarily to accommodate the filtering system. If the change in behavior is only temporary, then once the system stops blocking them, their unacceptable behavior would likely return.

Finally, the web filtering data can be aggregated into a user profile. The amount of time that passes between each occurrence in which the filtering modules are triggered can be analyzed. Such an

Table 6
Results of module-level analysis with controls for the non-SW location.

	Standardized coefficients		Collinearity statistics		Descriptive statistics		
	Beta	Sig.	Tolerance	VIF	Mean	Std. dev	*N*
Appropriate Use					84,210.54	86,998.80	70
Block	.360	.001***	.941	1.063	2206.16	5123.80	70
Confirmation	.441	.000***	.964	1.037	2645.37	5196.25	70
Quota	.134	.190	.911	1.098	2182.54	6655.19	70
Age	−.005	.970	.541	1.849	42.63	12.92	70
Tenure	.128	.325	.559	1.791	3686.43	3879.25	70
			Model fit				
Adjusted *R*-squared			0.3608	Std. error of the estimate			69,551.487

* = $p < 0.05$.
** = $p < 0.01$.
*** = $p < 0.001$.

analysis would provide evidence for the strength of the conditioning that occurs when users are prompted to use their quota time or mark a site as work related. As users' familiarity with the system increases, the amount of time between occurrences (i.e., appropriate use) is expected to increase. If users' initial interactions with warning pages are strong enough to affect their browsing habits for an extended period, then implementing an interactive web filtering system would be unnecessary, and a passive system with scheduled warnings alone would be sufficient. If a pattern of conditioning is observable from the increase in time between occurrences of cyberloafing, then the system is more effective at training employees than reinforcing behaviors.

7. Conclusion

With the increased connectedness in society via the Internet, the separation of personal time from work time is becoming blurred. Employees now use the computing resources of their organizations quite often for their personal use during work hours, which poses concerns about security, privacy, and productivity loss for organizations. In this paper, we explored and analyzed the effectiveness of a countermeasure for this cyberloafing problem involving a technical solution of Internet filtering and monitoring. Taking a multi-theoretical perspective, we employ operant conditioning and individuals' psychological morals of procedural justice and social norms to study the effectiveness of this countermeasure in addressing this agency problem of cyberloafing and in promoting greater compliance with an organization's Internet usage policies. In addition to the blocking module, our results show that confirmation and quota modules can prevent shirking and promote better compliance with Internet usage policies through employee empowerment and attention resource replenishment. Implications for practice and topics for future research are identified from our findings.

Acknowledgements

The authors thank Professors Raghu Santanam, Pei-yu Chen, Bin Gu, the anonymous reviewers, the AE, and the editor-in-chief for their constructive comments and insightful suggestions, which have greatly improved the lucidity of the paper. The usual disclaimer applies.

References

[1] G. Akerlof, A theory of social custom, of which unemployment may be one consequence, Q. J. Econ. 94, 1980, pp. 749–775.
[2] G.S. Alder, T.W. Noel, M.L. Ambrose, Clarifying the effects of Internet monitoring on job attitudes: the mediating role of employee trust, Inform. Manage. 43 (7), 2006, pp. 894–903.
[3] M.A. Al-Khaldi, R.S.O. Wallace, The influence of attitudes on personal computer utilization among knowledge workers: the case of Saudi Arabia, Inform. Manage. 36 (4), 1999, pp. 185–204.
[4] G.W. Bock, S.C. Park, Y. Zhang, Why employees do non-work-related computing in the workplace, J. Comput. Inform. Syst. 50 (3), 2010, pp. 150–163.
[5] S. Chai, S. Das, H.R. Rao, Factors affecting bloggers' knowledge sharing: an investigation across gender, J. Manage. Inform. Syst. 28 (3), 2011, pp. 309–342.
[6] T.Y. Chou, S.C.T. Chou, J.J. Jiang, G. Klein, The organizational citizenship behavior of IS personnel: does organizational justice matter? Inform. Manage. 50 (2–3), 2013, pp. 105–111.
[7] Y. Cohen-Charash, P.E. Spector, The role of justice in organizations: a meta-analysis, Organ. Behav. Hum. Decis. Process. 86 (2), 2001, pp. 278–321.
[8] B.L.S. Coker, Workplace Internet leisure browsing, Hum. Perform. 26 (2), 2013, pp. 114–125.
[9] J.A. Conger, R.N. Kanungo, The empowerment process: integrating theory and practice, Acad. Manage. Rev. 13 (3), 1988, pp. 471–482.
[10] G.S. Dawson, R.T. Watson, M. Boudreau, Information asymmetry in information systems consulting: toward a theory of relationship constraints, J. Manage. Inform. Syst. 27 (3), 2010, pp. 143–178.
[11] M.P. Domjan, The Essentials of Conditioning and Learning, 3rd ed., Wadsworth Publishing, Stamford, CT, 2004.
[12] K.M. Eisenhardt, Agency theory: an assessment and review, Acad. Manage. Rev. 14 (1), 1989, pp. 57–74.
[13] J. Elster, Social norms and economic theory, J. Econ. Perspect. 3 (4), 1989, pp. 99–117.
[14] B.S. Frey, I. Bohnet, Institutions affect fairness: experimental investigations, J. Inst. Theoretical Econ. 152 (2), 1995, pp. 286–303.
[15] D. Gefen, A. Ragowsky, C. Ridings, Leadership and justice: increasing non participating users' assessment of an IT through passive participation, Inform. Manage. 45 (8), 2008, pp. 507–512.
[16] M.L. Gruys, P.R. Sackett, Investigating the dimensionality of counterproductive work behavior, Int. J. Select. Assess. 11 (1), 2003, pp. 30–42.
[17] C.A. Henle, G. Kohut, R. Booth, Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing, Comput. Hum. Behav. 25 (4), 2009, pp. 902–910.
[18] R.A. Henning, P. Jacques, G.V. Kissel, A.B. Sullivan, S.M. Alteras-Webb, Frequent short rest breaks from computer work: effects on productivity and well-being at two field sites, Ergonomics 40 (1), 1997, pp. 78–91.
[19] P.E.N. Howard, L. Rainie, S. Jones, Days and nights on the Internet: the impact of a diffusing technology, Am. Behav. Sci. 45 (3), 2001, pp. 383–404.
[20] M.L. Jensen, W.H. Meckling, Theory of the firm: managerial behavior, agency costs and ownership structure, J. Financ. Econ. 3 (4), 1976, pp. 305–360.
[21] P.R. Johnson, C. Rawlins, Employee Internet management: getting people back to work, J. Organ. Culture Commun. Conflict 12 (1), 2008, pp. 43–48.
[22] G.R. Jones, Task visibility, free riding, and shirking: explaining the effect of structure and technology on employee behavior, Acad. Manage. Rev. 9 (4), 1984, pp. 684–695.
[23] R.M. Kanter, Power failure in management circuits, Harvard Bus. Rev. 57 (4), 1997, pp. 65–75.
[24] R.E. Kidwell, C.L. Martin, The Prevalence (and Ambiguity) of Deviant Behavior at Work, Managing Organizational Deviance, Thousand Oaks, CA, 2005.
[25] V.K.G. Lim, The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice, J. Organ. Behav. 23 (5), 2002, pp. 675–694.
[26] V.K.G. Lim, T.S.H. Teo, Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore – an exploratory study, Inform. Manage. 42 (8), 2005, pp. 1081–1093.
[27] E.A. Lind, T.R. Tyler, The Social Psychology of Procedural Justice, Plenum, New York, NY, 1988.
[28] H. Li, J. Zhang, R. Sarathy, Understanding compliance with Internet use policy from the perspective of rational choice theory, Decis. Support Syst. 48 (4), 2010, pp. 635–645.
[29] Y. Malhotra, D. Galletta, A multidimensional commitment model of volitional systems adoption and usage behavior, J. Manage. Inform. Syst. 22 (1), 2005, pp. 117–151.
[30] L. Minkler, Shirking and motivations in firms, Int. J. Ind. Organ. 22, 2004, pp. 863–884.
[31] C.J. Muhl, Workplace e-mail and Internet use: employees and employers beware, Monthly Labor Rev. 126 (2), 2003, pp. 36–45.
[32] L. Orans, P. Firstbrook, Magic quadrant for secure web gateways, Gartner Reports, 2013.
[33] J. Scott, G. Marshall, A Dictionary of Sociology, Oxford University Press, Oxford, 2009.
[34] S.K. Sharma, J.N.D. Gupta, Improving workers' productivity and reducing Internet abuse, J. Comput. Inform. Syst. 44 (2), 2003, pp. 74–78.
[35] B.F. Skinner, The Behavior of Organisms: An Experimental Analysis, Copley Publishing Group, Cambridge, MA, 1938.
[36] J.M. Twenge, S.M. Campbell, B.J. Hoffman, C.E. Lance, Generational differences in work values: leisure and extrinsic values increasing, social and intrinsic values decreasing, J. Manage. 36 (5), 2010, pp. 1117–1142.
[37] I.O. Ugboro, K. Obeng, Top management leadership, employee empowerment, job satisfaction, and customer satisfaction in TQM organizations: an empirical study, J. Qual. Manage. 5 (2), 2000, pp. 247–272.
[38] A. Urbaczewski, L.M. Jessup, Does electronic monitoring of employee Internet work? Commun. ACM 45 (1), 2002, pp. 80–83.
[39] D.A. Wilder, J. Austin, S. Casella, Applying behavior analysis in organizations: organizational behavior management, Psychol. Serv. 6 (3), 2009, pp. 202–211.
[40] H. Xu, H.H. Teo, B.C. Tan, R. Agarwal, The role of push-pull technology in privacy calculus: the case of location-based services, J. Manage. Inform. Syst. 26 (3), 2010, pp. 135–174.
[41] K. Young, Internet addiction: the emergence of a new clinical disorder, Am. Behav. Sci. 48 (4), 2004, pp. 402–415.
[42] K. Young, Policies and procedures to manage employee Internet abuse, Comput. Hum. Behav. 26 (6), 2010, pp. 1467–1471.
[43] F.R.H. Zijlstra, A.B. Leonova, R.A. Roe, I. Krediet, Temporal factors in mental work: effects of interrupted activities, J. Occup. Organ. Psychol. 72 (2), 1999, pp. 163–185.
[44] P. Zoghbi-Manrique-de-Lara, Inequity, conflict, and compliance dilemma as causes of cyberloafing, Int. J. Conflict Manage. 20 (2), 2009, pp. 188–201.

Jeremy Glassman is a PhD Student studying Information Systems in the W. P. Carey School of Business at Arizona State University. He received his B.S. from Arizona State University and his M.S. in Information Systems and M.B.A from the Eller School of Management at the University of Arizona. His research interests include IT resource usage in the enterprise, IS security, and agribusiness IT.

Marilyn Prosch is a Manager at Ernst & Young LLP in the National Advisory Practice. While conducting this research, she was an Associate Professor of Information Systems at Arizona State University. She has published in *The Accounting Review*, *Journal of Information Systems*, and *Journal of Forecasting*, among others.

Benjamin B. M. Shao is an Associate Professor of Information Systems in the W. P. Carey School of Business at Arizona State University. He received his B.S. and M.S. from National Chiao Tung University, Taiwan, and Ph.D. from the State University of New York at Buffalo. His research interests include IT impacts, IS security, healthcare IT, distributed collaborative systems, and software project management. He has published more than 65 refereed papers in leading journals and conference proceedings across the disciplines of Information Systems, Computer Science, Production and Operations Management, Operations Research, and Healthcare Management. He had served or is serving on the editorial boards of seven scholar journals including *Journal of the AIS, Decision Support Systems, Information & Management, Information Technology & Management*, and *MIS Quarterly* special issue. In the W. P. Carey School, he was recognized for teaching excellence as the DISC Professor of the Year and the finalist for the John W. Teets Outstanding Teaching Award.