Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2010 Proceedings

International Conference on Information Systems (ICIS)

2010

UNDERSTANDING THE EFFECT OF DETERRENCE MECHANISMS ON CYBERLOAFING: EXPLORING A GENERAL DETERRENCE MODEL WITH A SOCIAL PERSPECTIVE

Joseph C. Ugrin
Kansas State University, jugrin@ksu.edu

J. Michael Pearson
Southern Illinois University Carbondale, jpearson@cba.siu.edu

UNDERSTANDING THE EFFECT OF DETERRENCE MECHANISMS ON CYBERLOAFING: EXPLORING A GENERAL DETERRENCE MODEL WITH A SOCIAL PERSPECTIVE

Research-in-Progress

Joseph C. Ugrin
Kansas State University
Manhattan, KS 66506
jugrin@ksu.edu

J. Michael Pearson
Southern Illinois University Carbondale
Carbondale, IL 62901
jpearson@cba.siu.edu

Abstract

As the use of the Internet has grown, so have new ways for employees to loaf. Cyberloafing has become a pervasive problem for firms. Information systems researchers have suggested that a deterrence approach through the use of acceptable use policies for Internet-based applications coupled with Internet monitoring mechanisms can be an effective way to reduce cyberloafing without actively blocking websites and impeding on the positive aspects of the Internet. However, the effectiveness of the deterrence approach is still in question due to inconsistent results in existing research. This study aims to reconcile these inconsistencies by exploring how other factors interact with the deterrence model. We propose that the deterrence model will affect more deviant types of behaviors differently than those that are perceived to be more socially acceptable. We also suggest that employees will self-impose expected ramifications or sanctions on themselves when they expect to get caught cyberloafing.

Keywords: General Deterrence Theory, Cyberloafing, Internet Acceptable Use Policy, Stigma

Introduction

Internet resources have become important components of the workplace and can be beneficial to organizations (Whitty & Carr, 2006). Although they are being used to improve work performance, they can also be abused by using resources excessively for personal purposes. In the literature this has been coined cyberloafing, cyberslacking, non-work related computing or information systems misuse. Employees cyberloaf through activities like online shopping, personal investment management, emailing, and viewing traditional online media and pornographic materials (Blanchard and Henle, 2008; Lim, Teo and Loo, 2002) along with more recent developments such as social networking through websites like Facebook and MySpace (Ugrin and Pearson, 2008). Some have argued that many of these types of abuses are not new for employers who have struggled with loafing in many ways prior to the Internet (Block, 2001). But the Internet seems to exacerbate the loafing problem due to ease of access, the volume of information, and types of activities that can be performed over the net that are not available otherwise (Greenfield and Davis, 2002; Phillips, 2006). The Academic and popular press has published hundreds of articles illustrating the negative implications of cyberloafing; perhaps none more captivating than the recent scandal at the Securities and Exchange Commission involving dozens of employees who spent sizable amounts of their workday viewing pornography. That instance of abuse surprisingly involved both men and women and both high and low ranking employees (Simmons, 2010).

Some specific repercussions of cyberloafing for firms include lost time and productivity (George, 1996; Griffiths, 2003), loss of bandwidth (Firoz, Taghi and Souckova, 2006), and potential lawsuits resulting from severe forms of abuse like viewing and exposing others to sexual and pornographic material (Cohen, 2001). As such, many information systems researchers and professionals have suggested that organizations take a deterrence approach through the use of acceptable use policies (AUPs) for Internet-based applications (Dhillon, 1999; Parker 1998; Straub and Welke, 1998) coupled with Internet monitoring mechanisms (Siau, Nah, and Teng, 2002; Stiefer, 2000). They propose that the deterrence approach can be an effective way to reduce cyberloafing without actively blocking websites and impeding on the positive aspects of the Internet. AUPs aim to deter cyberloafing by including guidelines on appropriate Internet use and outlining potential sanctions for misuse. Monitoring mechanisms assist in enforcement of the AUP (Retkwa, 1996; Ugrin and Pearson, 2008). But the effectiveness of the deterrence approach is questionable considering that cyberloafing continues be a workplace problem and the results of existing research are inconsistent. For example, AUPs have been shown to influence abusive computer behavior in general through awareness of a policy and through their coupling with monitoring systems (Harrington, 1996) yet the threat of the formal sanctions that are typically included have actually been linked with increased Internet abuse (de Manrique Lara, 2006).

Motivated by inconsistencies in the existing literature, this study looks at the deterrence factors commonly included in an AUP through the lens of General Deterrence Theory (GDT), a widely used criminological theory that suggests that deterrence mechanisms such as sanctions and monitoring can reduce illicit behavior. A number of studies in information systems have attempted to use GDT to understand how cyberloafing and other forms of information systems misuse can be deterred (Straub, 1990; Pahnila, Siponen, and Mahmood, 2007; Herath and Rao, 2009; D'Arcy, Hovav and Galletta, 2009; Li, Zhang and Sarathy, 2010), but they have yielded mixed results and have provided limited support for GDT. We suggest that the disagreement amongst researchers is the result of two primary causes. The first is the failure to integrate the interactive effects of three mechanisms; sanctions, monitoring, and enforcement. Considering that GDT is a sanction based approach where sanctions are more effectual when they are more certain to be imposed, perceptions about certainty are influenced by the detection mechanisms that are in place and past enforcement activities. The second cause for the disparate findings is the failure to integrate personal standards and social norms into the GDT model (e.g. Paternoster and Simpson, 1996). We anticipate that sanctions will be less effective when an activity is perceived to be especially deviant (Polinsky and Shavell, 1999). We expect that highly deviant activities will tend to be influence by self imposed sanctions based on expected consequences from being branded or stigmatized from being caught abusing the Internet. Consequently, highly deviant activities will tend to be deterred to the extent that individuals perceive that they will get caught and others will find out about their behavior. If employers aim to deter activities that employees perceive to be more socially acceptable, they will need to formally impose sanctions like those outlined in an AUP. Although there have been limited investigations of this perspective[1], we propose that it may have particular relevance on

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

cyberloafing where different types of Internet usage are more socially unacceptable (e.g. viewing pornography) than others (e.g. personal emailing). Finally, we propose that perceived deviance is influenced by demographics, most notably age, where we anticipate that the acceptability of different types of non-work related Internet usage will vary between older and younger individuals and result in different degrees of self regulation and different effects of the GDT mechanisms on cyberloafing. Existing research has shown that younger individuals tend to cyberloaf more than older individuals (Ugrin and Pearson, 2007)

This study will use an experiment to test the effects of the GDT model and more interestingly, an expanded analysis that replaces imposed sanctions with perceived social ramifications and the effect of self-imposed sanctions that are not formally outlined in a policy (such as a firm's AUP) or law. This study diverges from recent applications of GDT to cyberloafing and will explain differences in the results of recent literature by examining the cyberloafing dilemma using a 'psycho-social' perspective that looks at how the psyche is influenced by not only the direct consequences of a traditional deterrence model that imposes sanctions, but also self-imposed consequences that are expected to come from the workplace and society. It illustrates how different types of cyberloafing are affected by deterrence mechanisms and how those effects are influenced by generational differences.

Hypotheses Development

Contrasting views to moral and ethical decision making seemingly converge when examining Internet usage in the workplace. Firms have approached cyberloafing from a teleological perspective by incorporating deterrence mechanisms to monitor and sanction inappropriate behavior. This lower order approach, driven by punishment and obedience, typically has the problem of not including all of the probable or significant consequences. For example, AUPs often include reference to specific sanctions; such as potentially getting fired, but cannot incorporate the effect of other social based sanctions that cannot be imposed by an employer directly. For example, one's perception that getting caught using the Internet inappropriately may lead to getting fired, but may also be harmful to one's future job prospects or result in social consequences due to the having the stigma of being a cyberloafer; perhaps even one that looked at socially unacceptable material. Whether or not ramifications on future employment and social related consequences are real or imagined is not particularly important. What is important is if they are perceived and self imposed into one's decision process; it's the perception that has the effect (Herath and Rao, 2009).

In addition to the effects of sanctions, real or perceived, consideration must be given to individual's personal views on whether or not an action is indeed dishonest or unacceptable. Higher order reasoning would suggest that a deontological perspective incorporating social roles and conformity driven by social contracts, along with personal virtues, would influence what types of behavior are considered abusive. Seemingly, individuals would consider how their Internet activities would fit into both the norms of society and their own personal virtues when deciding what types of activities are inappropriate. When abusive behaviors, as defined by an AUP, do not match those defined by employees, the AUP and its components may become less effective.

To test a deterrence model effectively, the model must incorporate both formally imposed sanctions, along with those that are expected to be imposed informally. It must also incorporate personal values and ethics that can influence those expectations.

The General Deterrence Model

General Deterrence Theory (GDT) is a criminological theory dating back centuries, and is the foundation for a large body of research in criminal justice, ethics, and recently, cyberloafing. GDT is based on an imposed regulatory model, emphasizing regulations that are placed on employees by organizations through the threat of sanctioning. GDT suggests that the threat of sanctions can modify employee actions when potential punishments are weighed against potential rewards for a specific behavior. The model relies on employees making rational decisions to benefit their current and/or future situations (Williams and Hawkins, 1986, Blair and Stout, 2001, Tyler and Blader, 2005, Willison, 2006). When confronted with opportunities and related consequences, individuals are rational actors who weigh the costs versus rewards of taking an action (Williams & Hawkins, 1986). This perspective on ethical decision making relies on individuals seeking outcomes that benefit themselves.

GDT has three components that are proposed to have an influence on illicit behavior; sanctions, detection, and enforcement. The primary factor in the GDT model is sanctioning. Sanctions are effective to the extent they are

deemed to be severe (D'Arcy et al., 2009; Ugrin and Odom, 2010). GDT is based on simple economic calculus where more punishment should equal more deterrence. In the context of cyberloafing, organizations with AUPs that threaten more severe punishment would theoretically see less cyberloafing. It is proposed that employees will be less likely to cyberloaf when the potential sanctions for cyberloafing are more severe.

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

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

H2: The effects of potential sanctions on cyberloafing will be more pronounced when monitoring mechanisms are present relative to no monitoring mechanisms.

A third question that can be raised is, "if organizations introduce potential sanctions for cyberloafing and monitoring mechanisms, will they work without enforcement?" In other words, the perceived likelihood of sanctions can be increased if people are aware that they are enforced after people are caught. We are not aware of research in the cyberloafing context that incorporates this facet into a GDT model. However, Lee and Lee (2002) did find that individuals are less likely to use company provided computers for inappropriate behavior when the individuals were aware of others being punished. But Lee and Lee (2002) failed to test if it was the awareness of enforcement that deterred individuals or the interactive effects between enforcement, detection, and the potential punishment. In two unrelated contexts, studies by Simpson and Koper (1992) and Ugrin and Odom (2010) examined the interactive effects of enforcement and sanctions. Simpson and Koper (1992) examined the impact of past guilty verdicts on reducing antitrust violations by corporations, finding that awareness of enforcement resulted in fewer violations and Ugrin and Odom (2010) examined the impact of the enforcement of sanctions for committing financial fraud on financial manager's attitudes about committing fraud, finding a three-way interaction between sanctions and enforcement when control mechanisms were in place. Although these studies are contextually unrelated and the Simpson and Koper study is at the firm level, they lend support for enforcement as a moderating factor in the GDT model.

Consequently, we expect that the effect of potential sanctions on cyberloafing will be moderated by employees' awareness of sanctions being enforced. We propose a three way interaction between potential punishment, monitoring, and enforcement. Punishment will be a strong deterrent if individuals expect to be caught and expect that the potential punishment will indeed be handed down. This can be likened to the following analogy related to highway speed limits. A speed limit alone may not deter a would-be speeder if there are no highway officers to monitor motorists' speeds or enforce regulations. In addition, the would-be speeder may still be undeterred if it is common knowledge that highway officers issue warnings rather than tickets. The same rationale can be used with other forms of illicit behavior, including cyberloafing.

H3: Monitoring mechanisms will moderate the effect of potential sanctions on cyberloafing to the extent that the potential sanctions are enforced.

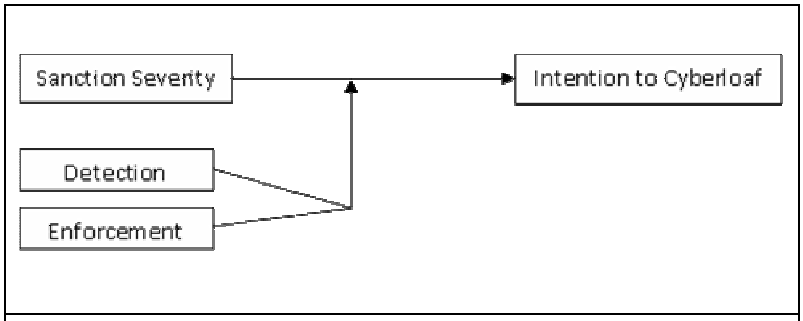

Figure 1. Deterrence Model

Self Imposed Factors: A Social Perspective to the Deterrence Model

Organizations that have implemented AUPs have essentially implemented an 'imposed' deterrence model; one that specifies what sanctions can potentially be leveled. In addition to the imposed deterrence model, theorists have argued that self regulation is a vital component of any deterrence effort (Tyler & Blader, 2005). "The self-regulated model emphasizes the role that employees' ethical values play in motivating rule following, and in particular those ethical values that are related to – and developed in the course of interactions – with their work organizations" (Tyler & Blader, 2005, p. 1149).

Ethical Alignment and Risk

The self-regulation model suggests that when individuals feel their organization is being managed with a sense of ethics that are in line with their own, they will feel compelled to behave in accordance with the policies and rules of the organization (Selznick, 1969; Aalders and Wilthagan, 1997; Gunningham and Rees, 1997; King and Lenox, 2000; Rechtschafen, 1998; Suchman, 1995; Tyler, 2001; Tyler and Darley; 1999; Tyler and Blader, 2005). This would seemingly hold true for Internet usage and the alignment between employee feelings toward cyberloafing and employer rules. Other research has shown in a variety of contexts that personal feelings or norms can have a moderating effect on the impact of deterrence factors on illicit behaviors, showing that deterrence factors are more effectual on more acceptable behaviors (Paternoster and Simpson, 1995; Li et al., 2010) and are more effectual on individuals who are less morally restrained (D'Arcy et al., 2009). This is consistent with other ethics literature that suggests that sanction based deterrence is a function of risk. In other words, if a behavior is not risky, there is little chance of being sanctioned (Cherry and Fraedrich, 2002). It seems difficult to rectify the conflicting results without examining various types of cyberloafing individually and existing studies (e.g. Li et al., 2010); de Manrique Lara, 2006; and D'Arcy et al., 2009) use either single scale or a composite score to test intentions in general, not intentions for specific behaviors such as using the Internet for sending personal emails versus using the Internet to view pornography.

Additionally, research has shown that employees feel Internet usage at work should be for both work related and non-work related activities (Whitty, 2002, 2004), potentially creating mis-alignment between employer and employee values and feelings of right and wrong. If that is the case, deterrence mechanisms must be in place if an employer aims to reduce Internet activities that are deemed acceptable by employees.

H4: The proposed deterrence model (H1, H2 and H3) will be more effectual on behaviors that are perceived to be less abusive as compared to behaviors that are perceived to be more abusive.

Self-Imposed Sanctions

The analysis of deterrence mechanisms can be expanded to examine the effects of self imposed factors like perceived social implications and long-term career effects. Other justice related research has found that the expected long-term effects of getting caught performing an illicit act, creating a 'stigma', can be a strong deterrent that works in conjunction with imposed sanctions (Ugrin and Odom, 2010). The costs of stigmas are internalized and incorporated into one's beliefs about the cost versus benefit of an illicit act and thus influence attitudes and behavior

just as any formal sanction would. In the case of socially unacceptable behavior, sanctions can have large effects at even small levels if the perpetrator perceives that a result of the sanctions will lead to important others finding out about the offense and the offender being socially stigmatized and ostracized or devalued. Polinsky and Shavell (1999) would argue that devaluation creates a disutility for an illicit act which would be especially true for risk averse individuals or with risky[2] behaviors. Ugrin and Odom's (2010) findings suggest that when individuals are caught committing an illicit act in the workplace, they feel their career will be negatively affected regardless of actual sanctions imposed. Both of these studies lend credence to our argument that perceived implications of being stigmatized serve as a self imposed sanction even though Polinsky and Shavell's paper is theoretical and both are in different contexts. For example, Ugrin and Odom (2010) examine what the effects of being caught committing financial reporting fraud will have on future employment and Polinsky and Shavell (1999) examine the effects of stigmas on convicted felons. Ugrin and Odom's (2010) study is also limited in how stigmas are measured since they use utilize single items to attempt to capture job related stigmas and social related stigmas and they don't really measure the underlying construct that drives behavior, the devaluation that comes from being stigmatized. Regardless, these studies suggest that perceived future stigmas play a role in the effectiveness of deterrence mechanisms.

H5: Intentions to cyberloaf will be lower when expectations of stigmas are higher.

Like formal sanctions, devaluation that arises from being branded with a stigma should deter cyberloafing in conjunction with other mechanisms such as monitoring and enforcement that would tend to increase the chance that significant others will find out about their Internet activities.

H6: The deterrence effect of expecting to be devalued due the stigma created by being caught performing various forms of cyberloafing will be more pronounced in the presence of monitoring mechanisms relative to no monitoring mechanisms.

H7: Monitoring mechanisms will moderate the effect of expected devaluation on cyberloafing to the extent that participants are aware that others have been sanctioned.

However, we also propose that the effects of expected devaluation due to a stigma will be more influential on more socially unacceptable types of behavior, like viewing pornography, and not as much for behaviors that are accepted (e.g. personal emailing). This is contrary to our discussion leading into H4. The rationale behind this is that potential social ramifications due to being stigmatized are only self imposed when a behavior is perceived to be socially unacceptable which is in contrast to socially acceptable behaviors that do not result in self imposed sanctions and require imposed sanctions if behavior is to be influenced.

H8: The effect of expected devaluation on cyberloafing intentions will be more effectual for behaviors that are socially unacceptable.

Methodology

Participants and Descriptive Statistics

We have planned to collect data from graduate students in business and employees at several firms in a diverse set of industries. It has been shown that business students can be good proxies for professionals in an ethical setting (Cohen, Pant, and Sharp, 2001). But in this domain we expected that differences in age, where younger individuals have been shown to be more prone to cyberloaf (Ugrin and Pearson, 2007), may result in different perceptions about Internet abuse and thus may result in differing tendencies towards cyberloafing and differing reactions to mechanisms aimed at deterring cyberloafing.

The Experiment and Measurement of the Primary Variables of Interest

To test the research questions, an experimental survey using a 2x2x2 between subjects design will be administered and the primary research questions will be tested using a MANOVA. Participants will be randomly assigned one

[2] Risky behaviors is defined here as behaviors that are more likely to result in a stigma.

scenario containing a combination of three decision cues: sanctions, monitoring mechanisms and enforcement. This type of scenario based methodology is widely used in ethics research (Weber, 1992). The manipulated cues represent two levels of each of the GDT based factors expected to affect cyberloafing. The cues will be presented as follows: (1) policy stating that employees will either be fired for abusing the Internet in the workplace (strong punishment) versus a verbal reprimand (low punishment) for abusing the Internet in the workplace, (2) the existence or non-existence of a monitoring system, (3) a statement indicating that others have (enforcement) or have not (no enforcement) been punished for abusing the Internet in this company. The experimental design will result in eight sets of cue combinations.

As mentioned in the introduction, the dependent variable will be measured across the six types of cyberloafing; Online Shopping (SHOPPING), Money Management (MNYMGMT), Emailing (EMAIL), Social Networking (SOCIALMEDIA), Viewing Online Pornography (PORN), and Viewing Online Media (MEDIA). Intentions will be measured by asking participants if they would perform each of the behaviors under the conditions presented to them along with asking participants how they feel a referent other would behave. Responses will be collected on likert type scales. The reason for eliciting participants' perceptions about a referent other is that responses to ethical decisions are often biased by a "halo effect" where individuals do not reveal their true intentions when they are asked directly about actions that may have potential social ramifications, but project them on a referent other when asked how the other would respond (Beeler and Hunton, 2002; Clement and Krueger, 2000; Cohen, Pant, and Sharp, 1993; 2001; Mikulineer and Horesh, 1999; Ruvolo and Fabin, 1999; Smith, 1997).

Self imposed sanctions will be measured through participants' perceptions that they will be ostracized or devalued if others find out about their cyberloafing activities. To capture participant's perceptions of being ostracized due the stigma created by being caught performing various forms of cyberloafing, we will utilize the devaluation/discrimination beliefs scale (Link et al., 1989), a 12-item instrument encompassing various facets of how participants can perceive that others will react to their stigma. Similar to Winnick and Bodkin (2008), we will change the original referent from "a former mental patient" to "someone caught abusing the Internet at work."

Finally, to measure how abusive participant's feel each type of Internet usage is in the workplace, they will be asked to rate each type of Internet usage on a 100 point scale where '0 = not abusive' to '100 = highly abusive' and rank each type of behavior from '1 = least abusive' to '6 = most abusive'.

Covariates

Various factors could systematically influence results and we will collect measures to ensure they are evenly distributed across treatment conditions. Individual's inherent levels of self-control (individuals low in self-control are less likely to control the urge to engage in illicit behavior) and responsibility denial (individuals that rate high in responsibility denial tend to depersonalize illicit acts and place responsibility on others) could influence the outcomes. Self-control will be measured by a 24-item 5-point Likert type scale developed by Grasmick et al. (1993) and further validated by Nagin and Paternoster (1993). Responsibility denial will be measured by a 28-item 5-point Likert type scale developed by Schwartz (1973, 1977) and additionally validated by Harrington (1996).

Beyond traits, moral decisions are a function of identification, e.g. whether or not the morality of a dilemma is identified (Rest, 1979). One would expect participants could be more apprehensive about cyberloafing if they recognize its influence on the organization. To measure that perception, participants will be asked if "using the Internet for personal purposes at work harms firms?" (1 = does not harm and 7 = is very harmful)

It seems plausible that general perceptions about the severity of typical punishments for cyberloafing could bias participants responses, thus perceptions about workplace sanctions in general will be measured by asking participants if "in general, punishment for Internet abuse at work is typically not severe (1) to severe (7)". Outcomes could also be affected by the perceived likelihood that control mechanisms are functional and would actually result in making sanctions more certain. Participants will be asked, "in the scenario previously described, would it be likely that you would get caught if you abused the Internet at work?" (1 = not likely to 7 = highly likely).

Finally, it can be conjectured that the perceived likelihood that monitoring mechanisms are effective may be affected by how closely participants perceive IT staff reviews data produced by Internet monitoring mechanisms and the volume of Internet traffic firms monitor. Participants will be asked if "data from Internet monitoring mechanisms typically monitored by IT staff" (1 = not very closely to 7 = very closely) and "the volume of Internet traffic that flows through firms relative to IT staff size is" (1 = very little traffic to 7 = high amount of traffic).

Manipulation Checks

Participants will answer three manipulation checks to ensure they understood the cue manipulations. The manipulation checks will be: "the company's Internet use policy states that you can be fired (verbally reprimanded) for abusing the Internet in the workplace", "the company employs (does not employ) a system to monitor your Internet activity" and "the company has (has not) punished others for abusing the Internet in the workplace."

Summary

The study will shed light on how individuals form their perceptions about Internet usage and what types of factors they take into account when considering different types of Internet activities in the workplace. We expect that the types of Internet usage that participants perceive to be less acceptable, will tend to be influenced by self imposed sanctions and perceived social ramifications more than behaviors that are felt to be more acceptable. As such, imposed mechanisms will be needed to deter acceptable activities. This may be a potential answer to the disparate findings among deterrence based studies which tend to treat all types of cyberloafing similarly when in reality, individuals' views on abusiveness may not match the views of their firms and their firms' AUPs. From a practical perspective we expect that merely the threat of monitoring can be an effective deterrent for highly unacceptable behaviors like viewing pornography but must be coupled with imposed sanctions and active enforcement to have an effect on other less deviant activities. Making employees aware of detection mechanisms may effectively cause them to consider ramifications like social stigma and create their own self imposed deterrence model if they feel the behavior is particularly unacceptable. But if a firm wants to reduce socially acceptable behaviors, more extreme actions must be taken, and sanctions must be imposed and made real.

References

Aalders, M. and Wilthagen, T. 1997. "Moving beyond command and control: reflexivity in the regulation of occupational safety and health and the environment," *Law and Policy* (19), 415-443.

Beeler, J. D. and Hunton, J. 2002. "Contingent economic rents: Insidious threats to audit independence," *Advances in Accounting Behavioral Research* (5), 21-50.

Blair, M. and Stout, L. 2001. "Trust, trustworthiness, and the behavioral foundations of corporate law," *University of Pennsylvania Law Review* (149), 1735-1810.

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

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

Cherry, J. and Fraedrich, J. 2002. "Perceived risk, moral philosophy and marketing ethics: mediating influences on sales managers' ethical decision-making." *Journal of Business Research* (55:12), 951-962.

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

Cohen, A. 2001. "Worker watchers." *Fortune* (143:13), 70-75.

Cohen, J., Pant, L. and Sharp, D. 1993. "Validation and extension of a multidivisional ethics scale," *Journal of Business Ethics* (12), 13-26.

Cohen, J., Pant, L. and Sharp, D. 2001. "An examination of the differences in ethical decision-making between Canadian business students and accounting professionals," *Journal of Business Ethics* (30), 319-336.

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

Dhillon, G., 1999. "Managing and controlling computer misuse," *Information Management and Computer Security* (7), 171-175.

Firoz, N., Taghi, R. and J. Souckova. 2006. "E-Mails in the workplace: The electronic equivalent to DNA evidence," *Journal of American Academy of Business* (8), 71-78.

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

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

Greenfield, D. N. and R. A. Davis. 2002. "Lost in cyberspace: the web at work," *CyberPsychology and Behavior* (5:4), 347-353.

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

Gunningham, N. and Rees, J. 1997. "Industry self-regulation," *Law and Policy* (19), 363-414.

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

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

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

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

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

Lim, V., Teo, T. and Loo, G. 2002. "How do I loaf here? Let me count the ways," *Communications of the ACM* (45:1), 66-70.

Link, Bruce G., Francis T. Cullen, Elmer Struening, Patrick E. Shrout, and Bruce Dohrenwend. 1989. ''A Modified Labeling Theory Approach to Mental Illness,'' *American Sociological Review* (54), 400-423.

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

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

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

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

Pahnila, S., Siponen, M., and Mohmood, A. 2007. "Employees' behavior toward IS security policy compliance," *40th Hawaii International Conference on Systems Sciences*, Hawaii.

Parker, B. 1998. *Globalization and Business Practice: Managing across Boundries,* Sage Publications.

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

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

Polinsky, A. and Shavell, S. 1999. "On the disutility and discounting of imprisonment and the theory of deterrence," *Journal of Legal Studies* (28:1), 1-16.

Rechtschaffen, C. 1998. "Deterrence vs. cooperation and the evolving theory of environmental enforcement," *Southern California Law Review* (71), 1181-1272.

Rest, James. 1979. *Development in Judging Moral Issues*. University of Minnesota Press.

Retkwa, R. 1996. "Corporate censors," *Internet World* (September), 60-64.

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

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

Schwartz, S. 1977. "Normative influences on altruism," *In Advances in Social Psychology*, L. Berkowitz (ed.), Academic Press, New York, 221-279.

Selznick, P. 1969. *Law, Society, and Justice*, New York: Russell-Sage Foundation.

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

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

Siau, K., Nah, F., and Teng, L. 2002. "Acceptable Internet use policy," *Communications of the ACM* (45:1) 75-79.

Simpson, S. S. and Koper, C. S. 1992. "Deterring corporate crime," *Criminology* (30:3), 347-375.

Stiefer, S. 2000. "Developing sensible e-mail and internet use policies," *Assessment Journal* (March-April), 53-56.

Straub, D. W. 1990. "Effective IS security: An empirical study," *Information Systems Research* (1:3), 255-276.
Straub, D. W. and Nance W. D. 1990. "Discovering and disciplining computer abuse in organizations: a field study," *MIS Quarterly* (14:1), 45-62.
Straub, D. W. and Welke, R. 1998. "Coping with systems risk: Security planning models for management decision making," MIS Quarterly (22:4).
Suchman, M. 1995. "Managing Legitimacy: strategic and institutional approaches," *Academy of Management Review* (20), 571-610.
Tyler, T.R. 2001. "Trust and law abidingness: a proactive model of social regulation," *Boston University Law Review* (81), 361-406.
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* (48:6), 1143-1158.
Tyler, T.R. and Darley, J.M. 1999. "Building a law-abiding society: taking public views about morality and the legitimacy of legal authorities into account when formulating substantive law," *Hofstra Law Review* (28), 707-739.
Ugrin, J. and Odom, M. 2010. "Exploring the Sarbanes-Oxley Act and Intentions to Commit Financial Statement Fraud: A General Deterrence Perspective," *Journal of Accounting and Public Policy* (29:5).
Ugrin, J. and Pearson, J. 2007. "Profiling cyberslackers in the workplace: Demographic, cultural, and workplace factors," Journal of Internet Commerce (6:3), 75-89.
Ugrin, J. and Pearson, J. 2008. "Exploring Internet abuse in the workplace: how can we maximize deterrence efforts?" *Review of Business* (28:2), 29-40.
Urbaczewski, A. and Jessup L. M. 2002. "Does electronic monitoring of employee Internet usage work?" *Communications of the ACM* (45:1), 80-83.
Weber, J. 1992. "The empirical quest for normative meaning: Empirical methodologies for the study of business ethics," *Business Ethics Quarterly* (2:2), 137-160.
Whitty, M. T. 2002. "Big brother in Australia: privacy and surveillance of the internet in the Australian workplace," *Paper presented at the Internet Research 3.0: Net/Work/Theory*, Maastricht, the Netherlands, Oct. 13-16.
Whitty, M. T. 2004. "Should filtering software be utilized in the workplace? Australian employees' attitudes towards internet usage and surveillance of the internet in the workplace," *Surveillance and Society* (2:1), 39-54.
Whitty M. T. and Carr A. N. 2006. "New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace," *Computers in Human Behavior* (22), 235-250.
Williams, K. R. and Hawkins, R. 1986. "Perceptual research on general deterrence: a critical review," *Law and Society Review* (20:4), 545-572.
Willison, R. 2006. "Understanding the perpetration of employee computer crime in the organizational context," *Information and Organizations* (16:4), 304-324.
Winnick, T. and Bodkin, N. 2008. "Anticipated stigma and stigma management amongst those labeled 'ex-con'," *Deviant Behavior* (29:4), 295-333.