

# Cyberloafing in the workplace: mitigation tactics and their impact on individuals' behavior

Lara Khansa<sup>1</sup> · Reza Barkhi<sup>2</sup> · Soumya Ray<sup>3</sup> · Zachary Davis<sup>4</sup>

Published online: 8 September 2017  
© Springer Science+Business Media, LLC 2017

**Abstract** With the Internet permeating every aspect of daily life, organizations of all types are increasingly concerned about the degree to which their employees are cyberloafing by shirking their work responsibilities to surf the Internet, check e-mail, or send text messages. Although technological interventions against cyberloafing have been shown to be effective, they might be perceived by employees as an invasion to their privacy, and are expected to have repercussions on employee behavior and loyalty. The main objectives of this study are to (1) examine how the introduction of such technological interventions might

affect employees' emotions and fairness perceptions, and (2) understand the effect of the interventions on behavioral outcomes, i.e., employees' intentions to cyberloaf and their loyalty to the company. We developed a justice-based framework that we empirically test using a field experiment composed of field surveys complemented with hypothetical scenarios describing new organizational initiatives to curb employees' cyberloafing. Our findings suggest that technological interventions, although associated with perceptions of unfairness, are effective at controlling cyberloafing, albeit at the expense of employee loyalty. On the other hand, contrary to prior findings, we find that fairness perceptions of technological interventions, although reinforcing employee loyalty, are ineffective at curbing cyberloafing. These findings are especially enlightening in that they contradict a common belief that perceived fairness encourages employees, as a sign of their appreciation for this fairness, to curb their misuse of IT. The findings also help managers fine-tune their cyberloafing policies to achieve a long-lasting remedy to their employees' cyberloafing while maintaining a necessary level of employee loyalty.

**Electronic supplementary material** The online version of this article (doi:[10.1007/s10799-017-0280-1](https://doi.org/10.1007/s10799-017-0280-1)) contains supplementary material, which is available to authorized users.

✉ Reza Barkhi  
reza@vt.edu  
Lara Khansa  
larak@vt.edu  
Soumya Ray  
soumya.ray@iss.nthu.edu.tw  
Zachary Davis  
zached1@vt.edu

<sup>1</sup> Department of Business Information Technology, Pamplin College of Business, Virginia Tech, 1030 Pamplin Hall (0209), Blacksburg, VA 24061, USA

<sup>2</sup> Department of Accounting and Information Systems, Pamplin College of Business, Virginia Tech, 3090 Pamplin Hall, Blacksburg, VA 24061-0101, USA

<sup>3</sup> Institute of Service Science, College of Technology Management, National Tsing Hua University, Hsinchu 30013, Taiwan, People's Republic of China

<sup>4</sup> Department of Business Information Technology, Pamplin College of Business, Virginia Tech, 1007 Pamplin Hall (0235), Blacksburg, VA 24061, USA

**Keywords** Cyberloafing · Justice · Fairness perceptions · Loyalty intention · Organizational commitment · Affect

## 1 Introduction

Cyberloafing entails engaging in nonwork-related activities such as surfing the Internet, online gaming, or simply sending personal e-mails during regular work hours [2]. Cyberloafing has been traditionally looked at as a workplace deviance (e.g., [2, 40, 41, 47, 76, 78]), but it has also been shown to help break work monotony and stress due to

lack of variety in daily routines, long hours at work, or excessive workload (e.g., [3]). While cyberloafing might be perceived as a stress relief or a reinvigorating and well-deserved break by some employees, companies have feared the potentially resulting losses in employee efficiency and productivity and have attempted to use various cyberloafing-curbing measures such as Internet use policies and technological interventions (e.g., monitoring technologies) [25, 61, 69]. In the United States, the monitoring of employees' online activities is permitted by law and actually practiced in some workplaces [74]. Monitoring technologies are available but their use is not the norm given that these technologies can stir employees' feelings of resentment and induce retaliatory behavior [52]. The use of monitoring technologies can further raise fears that human discretion and conventional social norms of privacy are violated [74]. This lack of normative understanding and privacy oversight can lead to emotional distress and employee turnover [82]. Accordingly, managers need to understand whether and (if so) how using anti-cyberloafing technologies is effective at reducing cyberloafing, while potentially causing other dysfunctional workplace behaviors and outcomes.

Research has found that organizational interventions are for the most part effective at curbing cyberloafing behavior, but they are likely to backfire by activating employees' neutralization, i.e., their rationalization of their cyberloafing behavior as justifiable and excusable [11, 30]. One study finds that, individually, threat termination and detection mechanisms are effective deterrents against activities like viewing pornography, managing personal finances, and personal shopping, but must be coupled together and actively enforced to dissuade activities like personal emailing and social networking [67]. Another research develops and tests a model based on the theory of planned behavior, and verifies this model within the context of cyberloafing [5]. Specifically, the authors find that cyberloafing is a withdrawal behavior, and that the three predictors, i.e., subjective descriptive norms, cyberloafing attitudes, and perceived ability to hide cyberloafing, predict cyberloafing behavior. A study by Cheng et al. [11] finds that the perceived benefits of cyberloafing have a positive effect on personal use of the Internet; specifically, perceived detection certainty has a negative effect on personal use of the Internet, while the effect of the severity of perceived sanctions on personal Internet use is not significant [11]. A study that focuses on two control methods, namely Internet use policies and electronic monitoring, shows that both methods can significantly lower employees' cyberloafing intentions; specifically, an Internet use policy is more effective for employees with a high level of self-esteem than it is for those with a low level of self-esteem; and similarly, electronic monitoring is more

effective for employees with a high level of job satisfaction than it is for those with a low level of job satisfaction [72]. Although this stream of research helps us understand employees' justifications better, it does not offer any strategies to avoid potential dysfunctions of cyberloafing and how management can enhance employee effectiveness and efficiency in the workplace. Another stream of research has investigated the antecedents of employees' cyberloafing [25, 30, 39, 61, 69]. For example, Khansa et al. [30, p. 165] found that "the announcement of formal controls activates the deterring influence of perceived risk on cyberloafing, but it also has the undesired effect of simultaneously actuating neutralization." They also mention that following the announcement of anti-cyberloafing organizational interventions, "other notable evaluations, both cognitive (e.g., perceived justice) and emotional (e.g., anger), also unexpectedly turned into significant precursors of cyberloafing intention" [p. 165]. However, the authors did not demonstrate how perceived fairness of organizational interventions affects employee loyalty. Taken together, the literature has paid little attention to the impact of organizational strategies and technological controls to address behaviors related to cyberloafing and employee loyalty.

The main objectives of this study are to (1) examine how technological interventions affect employees' fairness perceptions and affective reactions (e.g., emotions), and (2) to understand the effects that interventional factors have on behavioral outcomes such as cyberloafing intention and loyalty. To achieve these goals, we draw on interactional justice theory to explain employees' psychological reactions to general anti-cyberloafing technological interventions, including both their cognitive and affective responses. This allows us to understand the underlying antecedents of employees' justice perceptions and eventually predict their behaviors after the implementation of the technology to discourage cyberloafing. In addition, drawing on prior literature, we focus on factors that are rarely mentioned within the justice framework but that nevertheless play important roles in behavioral outcomes following after the implementation of such technology. The literature suggests that cyberloafing tendencies prior to the implementation of anti-cyberloafing technological interventions is an important antecedent of cyberloafing intention after technological interventions have been put in place [32, 33, 71]; on the other hand, organizational commitment has been established as a major antecedent of organizational loyalty [14, 59]. Our model extends the justice framework by including important conditions that are especially relevant for the discussion of both, cyberloafing and loyalty within the context of cyberloafing prevention. Overall, this study presents mechanisms through which a technological intervention influences individuals' cognitive and affective

reactions, and demonstrates how such reactions regulate behaviors after implementing anti-cyberloafing technological interventions.

This study contributes to cyberloafing and justice research in several ways. It is the first attempt to examine the role of a technological intervention in curbing cyberloafing by influencing individuals' behaviors in the workplace. In doing so, this study goes beyond merely identifying the determinants of employees' cyberloafing by investigating individuals' reactions to the introduction of new privacy-threatening technologies in the workplace. Second, this study extends justice theories by explaining how cognitive and affective responses to a technological intervention interact to form an overall evaluation of the justice of a cyberloafing-related situation. Third, this study is meaningful in that it explicitly examines how work conditions before implementing anti-cyberloafing technological interventions can set the stage for beliefs, feelings, and behaviors that are likely to materialize after interventions aiming at curbing cyberloafing are put in place. Much research has examined individuals' reactions to various organizational controls, but research is lacking that attempts to elucidate how, after the implementation of technological controls, interactional justice, context, and employees' commitment and affective reactions impact cyberloafing intentions and loyalty. Finally, we offer an investigation of two contrasting intentions, i.e., cyberloafing and loyalty, and assess the differential effect of a privacy-threatening technology on those behaviors. Thus, our study offers a fairly comprehensive picture of both desirable and unexpected consequences of a technological intervention to curtail cyberloafing.

The remainder of this paper is organized as follows. In the next section, we develop our hypotheses and the resulting model. We then present our data and variables, and measurement model. In the subsequent section, we report our results. We conclude by discussing the research insights and contributions of the study, its limitations, and potential avenues for further research.

## 2 Theoretical framework and hypotheses

Figure 1 shows a conceptual model that describes the impact of a technological intervention on individuals' perceptions and behavior. This model is intended to explain the extent of employee cyberloafing and loyalty intentions upon announcement of a formal technological intervention to thwart cyberloafing. In particular, our focus is on whether employees feel treated with respect and dignity in their organization's attempt to curb cyberloafing, rather than on issues of compensation. Unlike compensation and its related processes that are generally straightforward,

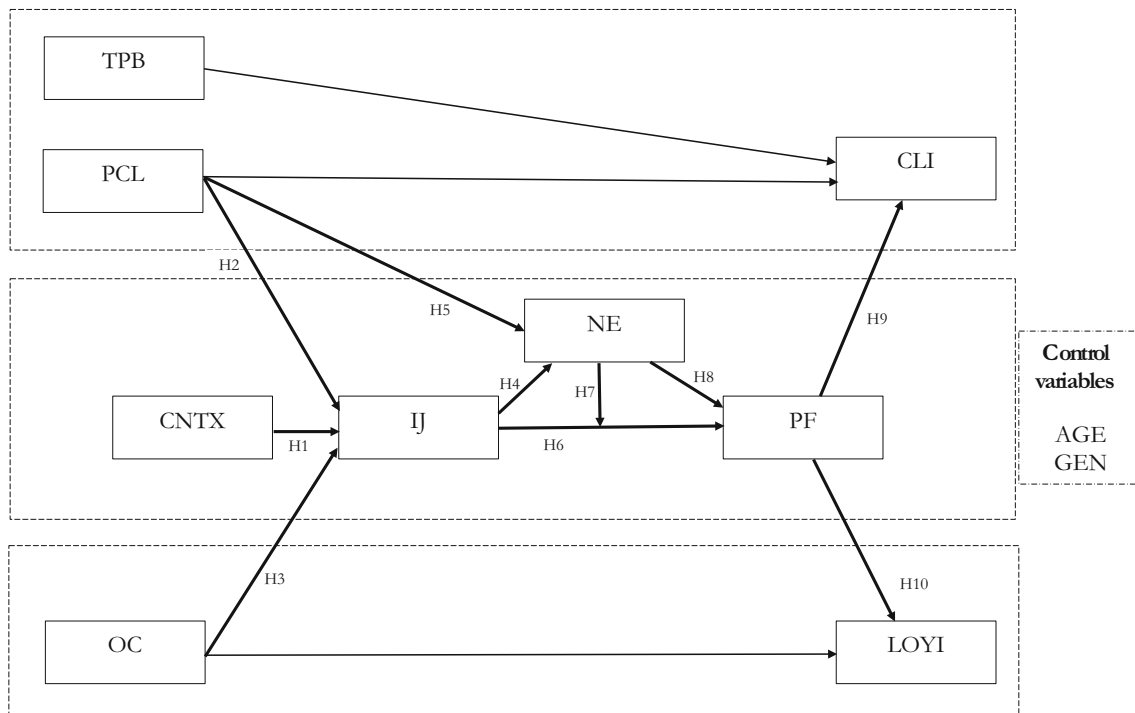
feelings about interpersonal treatment are subtle and complex, and could thus have far-reaching ramifications on employee morale, productivity, and even retention. Thus, it is important to assess how implementing technology to curb cyberloafing could impact employees from an interpersonal perspective.

Our model consists of three different, yet related, mechanisms, each of which is represented as a dotted rectangle in Fig. 1. At the top third of our conceptual model, an extended version of the theory of planned behavior (TPB) [1] is depicted. In general, the extended TPB model posits that future behavior is a function of not only traditional TPB factors (e.g., attitudes, subjective norm, and perceived behavioral control) but also past behavior [71]. In our context, it suggests that cyberloafing can be explained by TPB factors and past cyberloafing behavior. Meanwhile, in the bottom third of our conceptual model, Fig. 1 depicts the relationship between organizational commitment and employee loyalty. In the management literature, organizational commitment is well known as the major driver of organizational citizenship behavior including employee loyalty [75]. Consistent with the management literature, our model indicates that organizational commitment determines employee loyalty. Finally, the rectangle in the middle portion of our model shows that individuals' psychological responses to an organizational intervention can be represented as interactional justice, negative affective emotions, and fairness perceptions [18, 53]. CNTX in Fig. 1 refers to the way that the management team chooses to implement the anti-cyberloafing organizational intervention, i.e., whether they will formally monitor and punish cyberloafing behavior, or simply rely on employees' self-monitoring without formal monitoring and punishment. Please refer to Table 1 for the theoretical definitions of our measures.

Our model posits intermechanism relationships by suggesting that past cyberloafing and organizational commitment, along with technological context, determine individuals' psychological responses, which, in turn, influence subsequent cyberloafing and employee loyalty. Overall, in our model, drawing on the interactional justice theory, we capture individuals' psychological responses to the implementation of a privacy-threatening technological intervention through using interactional justice, negative affective reaction (e.g., emotions), and perceived fairness [14].

### 2.1 Interactional justice

The justice perspective has been used as a theoretical lens to understand a myriad of interactions ranging from customer-merchant relationships [7, 9, 13, 57] to interfirm relationships [35], and has been proven especially useful in



**Fig. 1** Research model. Bold paths were hypothesized.  $N = 552$ ; \* $p < 0.05$ , \*\* $p < 0.01$ , \*\*\* $p < 0.001$ . *CNTX* context, *AGE* age, *GEN* gender, *ATT* attitudes, *SN* subjective norm, *PBC* perceived behavioral

control, *PCL* past cyberloafing, *OC* organizational commitment, *IJ* interactional justice, *NE* negative emotions, *PF* perceived fairness, *CLI* cyberloafing intention, *LOYI* loyalty intention

assessing the nature of the interaction between employees and employers [14]. This is because in the workplace environment, employee performance, satisfaction, and subsequent attitudes and behavior have been directly linked to the degree of justice that employees perceive in the organizational practices and policies directed at them [62, 72, 78]. The introduction of organizational policies or technological interventions to enhance security and productivity can influence employee privacy and induce system restrictiveness that can negatively impact loyalty [59]. Employees will appraise the equitability of a privacy-threatening technology through the lens of justice, which is considered an essential component of any exchange relationship.

In the context of cyberloafing prevention, the way that managers utilize technology to curb cyberloafing can influence employees' evaluation of the intervention. Culpnan and Bies [15] identified three types of justice perceptions: distributive, procedural, and interactional.<sup>1</sup> Whereas, distributive justice is related to how fairly compensation is

distributed among employees, procedural justice is concerned with how compensation is determined [14]. Meanwhile, interactional justice addresses the extent of trustworthiness, responsiveness, and respectability that employers exhibit toward employees when they deliver organizational guidelines [62]. Consider the situation where employers clearly make their employees aware of new anti-cyberloafing guidelines through the installation of surveillance cameras in every office to track every employee's working habits and routines. In this scenario, employers have exhibited sufficient procedural justice when they have made employees aware of the company's guidelines by installing cameras, and have given them control over how they choose to behave. In this same scenario, however, employers showed a lack of interactional justice, i.e., "trustworthiness, empathy, and propriety" [62, p. 511] that are the three essential ingredients to achieve interactional justice. All in all, perceived organizational injustices are often not related to inadequacies in

<sup>1</sup> Organizational justice research defines three types of justice perceptions: distributive justice, i.e., the perceived fairness of outcomes, e.g., pay; procedural justice as the fairness of the "procedures used to determine one's outcomes" [18, p. 435], i.e., their "consistency, bias suppression, accuracy, correctability, representativeness, and ethicality" [18, p. 435]; and interactional justice as encompassing "various actions displaying social sensitivity, such as

Footnote 1 continued

when supervisors treat employees with respect and dignity (e.g., listening to a subordinates' concerns, providing adequate explanations for decisions, demonstrating empathy for the other person's plight)" [18, p. 435]. It is also widely recognized in organizational justice research "that a considerable proportion of perceived injustices did not concern distributional or procedural issues in the narrow sense but instead referred to the manner in which people were treated interpersonally during interactions and encounters" [18, p. 435].

**Table 1** Theoretical and operational definitions of main measures and constructs

Construct	Theoretical definitions	Operational definitions	Source
<i>Attitudinal variables (Input variables)</i>			
Organizational commitment (OC)	Organizational commitment refers to the extent of an employee’s involvement and identification with his or her organization	I am proud to be working for this organization I find that my values and those of the organization are very similar I feel loyal to this organization I am willing to work harder than I have to in order to help this organization succeed	[44]
Past cyberloafing (PCL)	The extent to which employees have cyberloafed in the past	On average, how frequently have you used the Internet at work for non-work-related purposes over the past month? (1 = less than once a week; 2 = a few times a week; 3 = about one a day; 4 = a few times a day; 5 = once an hour; 6 = several times an hour) I frequently use the Internet at work for non-work related purposes on a typical day	Newly developed
<i>Cognitive and affective variables (Intermediary variables)</i>			
Interactional justice (IJ)	The extent of trustworthiness, responsiveness, and respectability that employers exhibit toward employees when they deliver organizational guidelines	In the scenario described previously, the management team treats me in a kindly manner In the scenario described previously, the management team shows concern for my rights as an employee In the scenario described previously, the management team behaves in a way that fosters trust on my part	[53]
Perceived fairness (PF)	Employees’ overall perceptions of fairness	The management team is fair in this plan. This new plan is reasonable. I feel I am treated fairly by the management team	[55]
Negative emotions (NE)	Evoked feelings of fury, irritation, and anger	When you read the previous announcement by the organization, to what extent did you experience the following feelings? (1 = not at all to 7 = to a great extent) Furious Irritated Angry	[9, 54]
<i>Intentional variables</i>			
Cyberloafing intention (CLI)	Employees’ intentions to cyberloaf in the future	I predict that I would use the Internet at work for non-work-related purposes I intend to use the Internet at work for non-work-related purposes I plan to use the Internet at work for non-work-related purposes	[71]
Loyalty intention (LOYI)	Employees’ intentions to being loyal to their companies in the future	I will defend the organization when outsiders criticize it I will encourage friends and family to utilize the organization’s products and services I will stand up to protect the reputation of the organization	[16, 48]

distributive or procedural justice; rather, they have been attributed to problems in the manner that employees are treated “interpersonally” [62], i.e., interactional justice.

Organizational policies and controls are the rules, guidelines, and procedures that employers enforce to restrict their employees’ IT usage. Self-regulating controls or technologies, i.e., those that rely on employees’ “self-

regulating, self-monitoring, and self-sanctioning” [45, p. 85] have been shown to increase employees’ perceptions of accountability, while simultaneously improving employees’ perceived autonomy and empowerment [45] without being invasive or heavy handed [70]; these, in turn, replenish employees’ perceptions of interactional justice and encourage them to voluntarily align their self-interests

with those of their company. Unlike self-regulated controls, formal organizational interventions are those that monitor employees Internet usage, report Web usage to management, and suggest employees are likely to be subject to managerial sanction upon policy violation [70]. These formal controls that give the impression that employees may not determine their own use of technology violate norms of self-determination and autonomy that are fundamental needs for people [16, 25, 37, 45, 60, 70]. Because autonomy is such a key component of people's identity and motivation, employees view communications that threaten to take away their behavioral independence as contrary to the interpersonal aspects of interactional justice [14, 59].

Taken together, we believe that giving employees the autonomy to curb their cyberloafing behavior of their own volition by exercising self-regulating control, rather than through implementing formal monitoring, reporting, and sanctioning using formal organizational controls, instills in them perceptions of respect, self-worth, and ownership, and a feeling that management trusts them to do the right thing. Trustworthiness and respectability were shown to positively influence people's perceptions of interactional justice [62]. We therefore hypothesize the following:

**H1** Self-monitoring anti-cyberloafing technologies are positively associated with interactional justice.

Past behavior has been shown to serve as a reference point when people employ heuristics in the face of complex and unexpected situations [32, 33, 69]. In evaluating the social justice of change, people strongly rely on easy-to-access reference points to generate plausible alternative outcomes against which the proposed change can be judged [69]. In particular, recent experiences are useful reference points that can be used to evaluate new unfolding situations because recent experiences are easy to recall and are thus easier to simulate in subsequent scenarios and outcomes [32, 33, 69]. When a firm introduces a privacy-threatening technological intervention, recent past practices are the most accessible references against which employees can compare future outcomes. If employees have recently been able to cyberloaf, they exhibit disconfirmation when faced with new anti-cyberloafing measures [52, 69]. Thus, the more employees have engaged in cyberloafing before their organization intervenes, the more they will feel singled out and targeted when the technological intervention is announced, which in turn negatively influences their interactional justice perceptions. Such perceptions are likely to translate into a lower level of interactional justice. Thus, we expect that:

**H2** Past Cyberloafing will be negatively associated with interactional justice following the implementation of anti-cyberloafing technological interventions.

Organizational commitment refers to “the relative strength of an individual's identification with and involvement in a particular organization” [49, p. 226]. Mathews and Shepherd [46] added that committed employees exhibit a “strong belief in and acceptance of the organization's goals and values, show a willingness to exert considerable effort on behalf of the organization, and have a strong desire to maintain membership with the organization” [46, p. 369]. Zangaro [80] similarly explained that “a person who is committed to an organization should then be dedicated and have a strong belief in the organization's goals and values” [80, p. 14]. Such organizational commitment has been linked to readiness for and openness toward change in the workplace [73] and to organizational support in general [79, 80].

Organizational commitment toward the organization has been found to increase employees' acceptance of organizational change [28]. This is because employees' commitment aligns their interests and goals with those of the organization, and makes them more supportive of policies that are put in place in the best interest of the organization. Herscovitch and Meyer [26] explained that such organizational commitment generates “a force (mind-set) that binds an individual to a course of action deemed necessary for the successful implementation of a change initiative” [26, p. 475].

Following the same thought process, we propose that committed employees are likely to be more forgiving in their appraisal of the fairness of the interpersonal treatment, i.e., the interactional justice of the announcement of the organizational intervention. Let's assume for the sake of argument that we have two employees with different levels of (attitudinal) commitment toward the organization at the time of the announcement of the formal organizational intervention. We are proposing that the more committed employee will perceive higher levels of interactional justice in the way that the announcement was communicated. Although the announcement is the same for both employees, the level of interactional justice that the employees perceive the announcement to have depends on how committed they are to their organizations. This is akin to customers' exhibiting commitment (or loyalty in that case) toward a brand [51] and being more or less impervious to negative publicity of the brand; that is, at the time of the announcement of the negative publicity, customers' commitment (or loyalty in this case) toward the brand will affect how they internalize the same piece of negative news and how bad they perceive it.

All things considered, this suggests that committed employees are more likely to perceive anti-cyberloafing technological measures as exhibiting interactional justice, given that such policies are put in place to protect the company.

**H3** Organizational commitment will be positively associated with interactional justice following the implementation of anti-cyberloafing technological interventions.

## 2.2 Negative affective reaction

Individuals who feel they haven't been treated fairly are likely to experience negative affective reactions, i.e., a psychological state of anger or distress [52], toward those who cause the unfavorable situation. Justice research generally concurs on the view that individuals' evaluations of unfavorable situations produce both cognitive and affective responses [52, 54]. A cognitive response arises from one's deliberate calculation of whether the situation in question is in line with an implicit contract made between two parties [52, 57]. Meanwhile, affective responses originate from feelings of anger or distress concerning the way that someone has been treated by the other party [52]. According to the literature, interactional justice starts by a cognitive evaluation that triggers affective responses; Thus, we expect that lower perceptions of interactional justice following the implementation of a privacy-threatening technological intervention will lead to negative employee affective reactions.

Organizational research into affective responses has found that employees perceive interactional injustice as "hot and burning" and tend to be overwhelmed by feelings of anger as a result of this injustice [68]. Bies [8, p. 90] wrote that "the intense and personal pain associated with interactional injustice is experienced as a profound harm to one's psyche and identity—that is, one's sense of self." This indicates that interactional injustice is usually taken very personally and is prone to evoke a much more negative emotional response compared with the other two procedural and distributive injustices [72]. Taken together, we predict that lower perceptions of interactional injustice ignite negative affective reactions on the part of employees following the announcement of privacy-threatening technological measures.

**H4** The lower the interactional justice, the higher the negative affective reactions following the implementation of anti-cyberloafing technological interventions.

Employees who have engaged in cyberloafing in the past are likely to be those who see value in cyberloafing. They might rationalize their cyberloafing a way to get refocused to better do their jobs. These past cyberloafers have

probably found a way to rationalize cyberloafing as a legitimate activity, by finding an equitable balance between what they are getting from cyberloafing (entertainment, relaxation, completing their chores) and what they were offering their companies in terms of time and productivity [40].

Anti-cyberloafing policies and technologies restrict employees' nonwork-related activities, and increase expectations for higher work-related productivity. When cyberloafers are forced to give up what was once allowed without any accompanying compensation, they can experience disconfirmation, induced restrictiveness, and a feeling of unfairness [21, 68]. Moreover, because management introduces the new policy, employees will also consider these negative outcomes the result of managerial action and outside their immediate control. Negative results that emanate outside one's locus of control trigger negative affective reactions such as anger [9, 52, 57]. Therefore, any policy that seeks to curb cyberloafing will meet the sufficient criteria for triggering negative affective reactions especially among past cyberloafers. Thus, the more an employee has cyberloafed in the past, the greater the perceived loss and negative affective reactions following an anti-cyberloafing technological intervention.

**H5** The higher employees' past cyberloafing, the more negative affective reactions following the implementation of anti-cyberloafing technological interventions.

## 2.3 Perceived fairness

We earlier proposed that individuals' immediate reactions to a privacy-threatening technology take both cognitive and affective forms. In the context of IT use, user satisfaction is considered a psychological combination of cognitive evaluations and emotional feelings [34, 52, 54, 72]. In addition, customer attitudes are often used to characterize both cognitive beliefs and affective reactions in the context of customer behavior [7, 57].

Ample studies in the management literature have reported a significant impact of affect on judgement and intentions (e.g., [10, 58]). Campbell [10] reported that "people have affective reactions to many situations, that they monitor their feelings, and that their subjectively experienced affect influences higher-level evaluative judgments of various stimuli" [10, p. 262]. Particularly, the author showed that emotional reactions to pricing had a significant effect on perceived price unfairness. Other research has also demonstrated a significant causal influence of affect on evaluations and judgement such as fairness. Particularly, Xia et al. [77] showed a causal influence of emotional reaction on perceptions of fairness. Haidt [23] even showed that emotions influence perceived

(un)fairness more than cognitions. Finkel [17] also observed that unfairness perceptions have been found to result from “heat and passion, anger, and outrage” [17, p. 57]. This is because these affective reactions help people form initial responses to emerging situations and increase heuristic processing [70]; thus, affective reactions can sway the overall evaluation of an event one way or another [52, 57, 69]. Negative affective reactions often unfavorably bias a person’s overall judgment of the fairness of a new anti-cyberloafing technological intervention from the get go [35, 63]. It is thus reasonable to expect that employees’ negative affective reactions, following the implementation of a privacy-threatening technological intervention, will negatively influence their overall evaluation of the fairness of the intervention.

**H6** Negative affective reactions following the implementation of anti-cyberloafing technological interventions will negatively influence the perceived fairness of such intervention.

Employees evaluate how fairly they have been treated by their employers based on their perceptions of interactional justice [14]. Besides their fast emotional responses to the implementation of a privacy-threatening technological intervention, employees’ perceptions of interactional justice serve as an input to the formation of perceived fairness. Perceptions of interactional justice are not necessarily identical to judgments of overall fairness, but the former will certainly have a positive impact on the latter. Hence, we predict that higher appraisals of interactional justice will ultimately increase judgments of overall fairness.

**H7** The higher the interactional justice at the time of implementation of anti-cyberloafing technological interventions the higher the perceived fairness of using this technology.

Affective reactions moderate the effect of cognitive factors on overall perceptions. Individuals with negative affective reactions toward an event have been shown to be more sensitive to the process that managers use to convey their new policies [60]. Consequently, employees with negative affective reactions are more likely to carefully consider interactional justice in determining overall fairness. With these types of individuals, interactional justice is an even stronger determinant of the perceived fairness of their managers’ impositions. In our setting, employees would use their initial appraisals of interactional justice to judge the overall fairness of new policies promulgated to thwart cyberloafing. Hence, we predict that employees who are emotionally distressed with implementing cyberloafing technology will be stricter in their systematic appraisals of interactional justice. As such, we expect that negative affective reactions will positively moderate the relationship

between the appraisal of interactional justice and judgments of fairness.

**H8** As negative affective reactions increase (decrease), the relationship between interactional justice and perceived fairness gets stronger (weaker) following the implementation of anti-cyberloafing technological interventions.

## 2.4 Cyberloafing and loyalty

Throughout this paper, we have adopted the extant literature’s view that cyberloafing is a counterproductive behavior that distracts employees from the work they are paid to fulfill at their organization [39–41]. Cyberloafers have been shown to resort to neutralization techniques to rationalize their cyberloafing behavior. In particular, Khansa et al. [30] explain that the “metaphor of the ledger” neutralization technique “is often used by cyberloafers who argue that they are entitled to “cash in” on their previously impeccable employee behavior” (p. 145). The authors add that another neutralization technique, i.e., “denial of injury,” “has been found to be especially espoused by cyberloafers who use it to “downplay” or “trivialize” the consequences of their cyberloafing that, according to them, neither consumes time nor harms the organization.” (p. 145). Further, Khansa et al. [30] found that neutralization is only activated after the announcement of anti-cyberloafing interventions, but not before, because after the announcement “justification is needed to challenge the organization’s new stance on cyberloafing” (p. 152).

Based on these findings in the literature, we conjecture that when employees perceive the anti-cyberloafing measures to be fair, they are likely to downplay the negative effects of their cyberloafing [39, 61]); their justification would be that their organization does not believe cyberloafing to be detrimental because if it were, the organization would have imposed more stringent regulations. Further, with higher perceptions of fairness, the perceived risk of punishment is lower, which is likely to be less effective at reducing cyberloafing, as shown in [30]. The combination of decreased perceived risk of punishment and the increased neutralization together are expected to increase employees’ intentions to cyberloaf in the future. Taken together, we expect that:

**H9** Cyberloafing intention following the implementation of anti-cyberloafing technological interventions is positively related with perceived fairness.

Employees’ perceptions of fairness have been shown to play a critical role in shaping organizational citizenship behavior such as altruism, courtesy, conscientiousness, civic virtue, and sportsmanship [14, 59]. The literature



suggests that when facing unfair organizational measures, employees tend to counteract the perceived unfairness by reducing their goodwill without being overwhelmed by guilt [48]. Thus, if an organizational intervention is not perceived to be fair, individuals' loyalty toward their organization will dwindle. In the context of cyberloafing prevention, a privacy-threatening technology creates a sense of injustice that instills reduced employee loyalty intentions. Accordingly, we expect that perceived fairness is an important predictor of loyalty after *cyberloafing technology is implemented*. Thus,

**H10** Perceived fairness is positively related to loyalty intention following the implementation of anti-cyberloafing technological interventions.

In addition to the above hypothesized relationships, our proposed model controls for prior explanations of outcome factors. First, a prior study has adapted the theory of planned behavior to suggest that cyberloafing intentions can be fully explained as a planned behavior that arises from attitude, subjective norms, and perceived behavioral control [5]. Thus, our study also includes these three factors of the theory of planned behavior and controls for their effect on cyberloafing intentions. It is also well known that past behavior is a strong predictor of subsequent intention and behavior [22, 32, 33, 71], and, accordingly, past cyberloafing is specified to be a determinant of subsequent cyberloafing. Further, we include organizational commitment in the model as a major driver of organizational citizenship behavior (e.g., loyalty) [14, 59]. Finally, we also controlled for the effects of the demographic factors of gender and age on cyberloafing and loyalty intentions. Although these controlled relationships are not shown in Fig. 1, they will be estimated and reported in our analysis below.

### 3 Method and results

#### 3.1 Data collection

We employed a field experiment in which the characteristics of field surveys were complemented with hypothetical scenarios as experimental treatments. Specifically, a Web-based survey questionnaire was used to assess individuals' perceptions about cyberloafing and technology to monitor and prevent cyberloafing within their organization. Two different scenarios were prepared to estimate the role of information security policy contexts in regulating individuals' behaviors. In the survey questionnaire, a hypothetical scenario was presented that described a new organizational initiative to curb cyberloafing. Subjects were instructed to assume that such a technology was

actually announced at their organization. Overall, we measured individuals' perceptions and behavior specific to their real-life organization while manipulating information security policy contexts through hypothetical scenarios.

To conduct a survey, we worked with a market research firm that manages a nationwide online panel. We drew a sample frame of panel members between the ages of 20 and 65 who had a full-time or part-time job working at an organization at the time of the survey. We randomly selected 3000 U.S.-based members from the panel pool. E-mail invitations, each of which included a link to one of the two types of Web-based survey questionnaires, were sent to the potential subjects. They were informed that statistical analysis would be conducted only at the aggregate level and their personal information would be kept confidential. We collected a total of 611 responses but excluded 79 responses that indicated that their organization already adopted the technology mentioned in the scenario. As a result, we used 532 complete responses, which represented a response rate of 17.7%. The average age of subjects was 44, and 58% were male. To check for non-response bias, we compared the demographic profiles of respondents and nonrespondents but did not find any significant differences in terms of age and gender ( $p = ns$ ).

#### 3.2 Measures and scenarios

We conducted a literature review and identified measurement items in prior research and reworded them to suit the context of our study. The Appendix contains the specific items included in this study and Table 1 gives the operational definitions of the main constructs in the model. Our survey questionnaire consisted of three parts. Part A was intended to measure pre-intervention conditions, i.e., past cyberloafing and organizational commitment, and other potentially significant variables at the pre-intervention stage. Specifically, three factors discussed in the theory of planned behavior, namely: attitudes, subjective norm, and perceived behavioral control, were used as control variables. In particular, we used three items adapted from [65] to measure attitudes toward cyberloafing. The subjective norm was measured with two items borrowed from [71]. Four items adapted from [66] were used to measure perceived behavioral control. The scale of past cyberloafing, which included two items, was newly developed. Four items adapted from [44] were used to measure organizational commitment.

In Part B of the survey, a hypothetical scenario involved the implementation of an information security policy within the individual's organization. We developed two scenarios that differed with respect to the specific plans of the new information security policy. In the first scenario, respondents were asked to imagine that a weekly report

would be generated listing the websites the respondents visited and management would review the report. The second scenario was almost the same as the first, except that respondents were told that only they would receive the report of websites they had visited so that they know the cyberloafing technology would track their behavior while at the workplace. The scenarios were developed to address only interactional justice and exclude other types of justice (e.g., distributive justice, procedural justice) that are beyond the scope of our study. The first scenario in which management would review the report was coded as 1; the second scenario in which only the employee would review the report was coded as 2.

The third part of the survey, Part C, was designed to assess reactions to the policy described in the hypothetical scenario. The scales included interactional justice, negative emotions, perceived fairness, cyberloafing intention after the implementation of cyberloafing technology, and loyalty intention after implementing this technology. We used three items adapted from [53] to measure interactional justice. The three items of negative emotions were adapted from [9] and [54]. Perceived fairness was measured with three items that were based on the scale of global fairness in [55]. The scale of cyberloafing intention consisted of three items adapted from [71]. We measured loyalty intention by using three items adapted from [16] and [48]. Finally, we collected demographic information, such as age and gender, at the end of the survey questionnaire.

### 3.3 Measurement model

To assess the psychometric properties of the scales, we conducted a confirmatory factor analysis (CFA) using LISREL 8 [29]. Several different fit indices were used to evaluate various aspects of model fit [12, 21, 34]. The indices used in this were the comparative fit index (CFI), the nonnormed fit index (NNFI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR), the goodness-of-fit index (GFI), and the adjusted goodness of fit (AGFI). A model is considered acceptable if  $CFI \geq 0.95$ ,  $NNFI \geq 0.95$ ,  $RMSEA \leq 0.06$ ,  $SRMR \leq 0.08$ ;  $GFI \geq 0.90$ , and  $AGFI \geq 0.80$  [7, 21, 27]. Our measurement model included 13 factors with 32 indicators, including three one-item scales such as context, age, and gender. The results of CFA indicated that the measurement model fit the data satisfactorily:  $\chi^2(389) = 773.02$ ,  $p < 0.001$ ,  $CFI = 0.99$ ,  $NNFI = 0.99$ ,  $RMSEA = 0.043$ ,  $SRMR = 0.031$ ,  $GFI = 0.92$ ,  $AGFI = 0.89$ .

In addition to fit indices, we also examined the reliability, convergent validity, and discriminant validity of the scales. Table 2 shows the means, standard deviations, Cronbach's alpha (CA), composite reliability (CR),

average variance extracted (AVE), and correlations of the measures based on the measurement model. To measure the reliability of the scales, we used CA, CR and AVE. Reliability is considered acceptable if  $CA \geq 0.70$ ,  $CR \geq 0.70$  and  $AVE \geq 0.50$  [6, 19]. As indicated in Table 2, the CA, CR and AVE values exceeded the recommended values by significant amounts (i.e.,  $CA \geq 0.82$ ,  $CRs \geq 0.84$  and  $AVEs \geq 0.73$ ). We also checked the convergent validity of the scales. Convergent validity is said to be established if a standardized factor loading is greater than 0.60 [12]. Our examination into the output of LISREL 8 revealed that the lowest factor loading was 0.82 in the measurement model, which indicates satisfactory convergent validity of the scale measures. Meanwhile, the discriminant validity of the scales was examined through a series of Chi square difference tests for each pair of the factors [6]. For example, in examining the discriminant validity between interactional justice and perceived fairness, we compared proposed and alternative measurement models of the two constructs to confirm that their collective items are more appropriately modeled by two factors rather than a single factor. Specifically, we first constructed a proposed measurement model that allowed the three items of interactional justice and the three items of perceived fairness to respectively load upon separate reflective factors, with a free two-way association between the two factors. A goodness-of-fit test of this proposed measurement model yielded a Chi square of 30.14 with 8 degrees of freedom. In contrast, an alternative measurement model was also constructed wherein the six items of interactional justice and perceived fairness combined were only allowed to load upon a single factor. This alternative model yielded a Chi square of 477.48 with 9 degrees of freedom. We tested the discriminability of the proposed versus alternative model with a Chi square difference test (Chi square difference of 417.34 with 1 degree of freedom), which was significant at even 0.1%. Thus, we have evidence to support our proposition that interactional justice and perceived fairness are indeed significantly different factors. Similarly, we examined and confirmed the discriminant validity of all pairs of constructs. We also checked for potential multicollinearity, which is generally diagnosed by checking predictors for VIF values over 10 [24]. The VIF values for all our exogenous factors were well short of this threshold for critical multicollinearity. Overall, with acceptable model fit, reliability, convergent validity, discriminant validity, and multicollinearity, our scales were shown to exhibit desirable psychometric properties.

Because we collected the data from a single survey, the results of this study may suffer from common method variance (CMV). To assess the extent of CMV, we used the marker-variable technique [42, 43]. In this study, the scale

**Table 2** Properties of measurement scales

	ME	SD	VIF	CA	CR	AVE	Correlations			
							1	2	3	
1. CNTX	41.48	10.50	1.16	na	na	na	na			
2. AGE	44.20	12.06	1.31	na	na	na	−0.31***	na		
3. GEN	41.42	10.49	1.10	na	na	na	0.02	0.22***	na	
4. ATT	43.47	11.85	5.22	0.93	0.94	0.83	0.09*	−0.23***	−0.15***	
5. SN	43.80	11.99	4.19	0.95	0.95	0.90	0.07	−0.16***	−0.07	
6. PBC	44.20	11.97	2.50	0.91	0.91	0.77	0.07	−0.15***	−0.05	
7. PCL	42.99	11.76	3.49	0.82	0.84	0.73	0.09*	−0.29***	−0.08*	
8. OC	45.27	11.44	1.23	0.94	0.94	0.79	0.05	0.01	0.04	
9. IJ	44.25	11.72	4.84	0.93	0.94	0.83	0.20***	−0.13**	−0.00	
10. NE	42.73	11.76	1.70	0.92	0.93	0.82	−0.05	−0.11**	−0.13**	
11. PF	44.73	11.65	5.47	0.96	0.96	0.88	0.12**	−0.08*	−0.04	
12. CLI	43.28	12.02	na	0.98	0.98	0.94	0.14***	−0.16***	−0.08*	
13. LOYI	44.92	11.64	na	0.96	0.96	0.90	0.03	0.02	−0.09*	

	Correlations										
	4	5	6	7	8	9	10	11	12	13	
1. CNTX											
2. AGE											
3. GEN											
4. ATT	0.91										
5. SN	0.79***	0.95									
6. PBC	0.58***	0.68***	0.88								
7. PCL	0.74***	0.64***	0.61***	0.85							
8. OC	0.13**	0.19***	0.22***	0.12**	0.89						
9. IJ	−0.06	−0.03	0.05	−0.03	0.32**	0.91					
10. NE	0.38***	0.25***	0.14***	0.32***	−0.16***	−0.41***	0.91				
11. PF	−0.16***	−0.08*	0.02	−0.08	0.32***	0.85***	−0.52***	0.94			
12. CLI	0.72***	0.65***	0.54***	0.62***	0.14***	0.13**	0.20***	0.03	0.97		
13. LOYI	0.03	0.10*	0.16***	0.03	0.67***	0.48***	−0.31***	0.50***	0.20***	0.95	

ME mean, SD standard deviation, CA Cronbach’s alpha, CR composite reliability, AVE average variance extracted; *diagonals* square root of AVE. CNTX context, AGE age, GEN gender, ATT attitudes, SN subjective norm, PBC perceived behavioral control, PCL past cyberloafing, OC organizational commitment, IJ interactional justice, NE negative emotions, PF perceived fairness, CLI cyberloafing intention, LOYI loyalty intention

N = 532; \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

of fantasizing, which refers to the extent to which a person has a vivid imagination, was chosen as a marker variable [50]. This marker variable was deemed relatively irrelevant in the context of information security; accordingly, a correlation between fantasizing and other variables in this study could imply CMV. According to [42], the conservative estimate of CMV is inferred from the smallest correlation between the marker variable and other variables. We reran CFA by including the additional factor of fantasizing and found that the smallest correlation in absolute terms was close to 0 ( $r = -0.01, p = ns$ ).<sup>2</sup> These results indicate that CMV, if any, was unlikely to be significant in the present study. Taken together with the desirable

psychometric properties, our scales were found to be suitable for testing the structural model and research hypotheses.

### 3.4 Proposed and alternative models

We also used LISREL 8 as a structural equation modeling (SEM) tool to test the research model and hypotheses [29]. Table 3 and Fig. 2 present the results of the SEM analysis, which includes standardized path estimates and explained

<sup>2</sup> We reassessed a structural model after taking into account CMV and confirmed that the results of the hypotheses did not change.

**Table 3** Results of structural equation modeling

	IJ	NE	PF	CLI	LOYI
OC	<b>0.33</b> <sup>***</sup>				0.58 <sup>***</sup>
CNTX	<b>0.19</b> <sup>***</sup>				
PCL	<b>-0.09</b>	<b>0.33</b> <sup>***</sup>		0.17 <sup>**</sup>	
IJ		<b>-0.40</b> <sup>**</sup>	<b>0.76</b> <sup>***</sup>		
NE			<b>-0.21</b> <sup>***</sup>		
IJ * NE			<b>0.07</b> <sup>**</sup>		
PF				<b>0.13</b> <sup>***</sup>	<b>0.32</b> <sup>***</sup>
<i>Demographic controls</i>					
AGE				0.04	0.03
GEN				0.01	0.05
<i>Theory of planned behavior controls</i>					
ATT				0.46 <sup>***</sup>	
SN				0.12 <sup>*</sup>	
PBC				0.08	

Bold results were hypothesized

CNTX context, AGE age, GEN gender, ATT attitudes, SN subjective norm, PBC perceived behavioral control, PCL past cyberloafing, OC organizational commitment, IJ interactional justice, NE negative emotions, PF perceived fairness, CLI cyberloafing intention, LOYI loyalty intention

N = 532; \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

variance. First, the results of SEM showed that our model fit the data reasonably. In particular, the fit indices were well within the satisfactory ranges [ $\chi^2$  (444) = 943.38,  $p < 0.001$ , CFI = 0.99, NNFI = 0.98, RMSEA = 0.046, SRMR = 0.045, GFI = 0.90, AGFI = 0.88]. We found that all but one of the relationships specified in the model were significant at the 0.05 level (two-tailed). Moreover, our model was found to explain a significant amount of the variation in the outcome variables. Specifically, the model explained 57% of the variance in cyberloafing after technological intervention and 54% of the variance in loyalty after the technological intervention.

These results strongly suggest that our proposed model is a realistic representation of reality and a sound basis for the subsequent tests of research hypotheses. Of our major TPB control factors (ATT, SN, PBC), only attitudes significantly impacted CLI. Subjective norms had a surprisingly weak relationship with CLI, given the sample size of this study, while PBC was entirely insignificant. The impact of the demographic controls of age and gender were also insignificant. The relative lack of significance of our major controls is another indication of the overall efficacy of the conceptual model.

### 3.5 Tests of research hypotheses

In general, the hypotheses proposed in this study received strong support from the data; nine out of our ten hypotheses

were supported, and even the one exception was marginally supported. The specific results of the hypotheses are as follows:

#### 3.5.1 Interactional justice

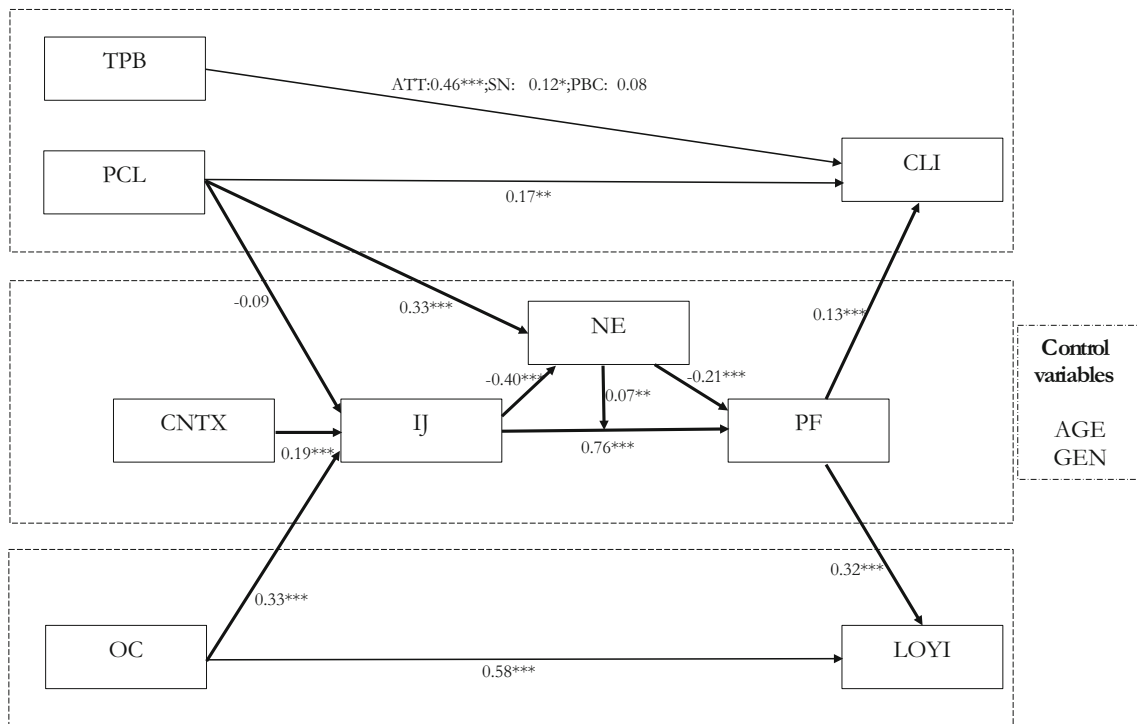
The first three hypotheses relate to the antecedents of interactional justice. First, we had proposed that the contextual difference would affect interactional justice. Consistent with this hypothesis, interactional justice was found to change with respect to the context of information security policy (parameter estimate = 0.19,  $p < 0.001$ , two-tailed; H1 supported). Second, we proposed that cyberloafing would relate negatively with interactional justice. As shown in Fig. 2, the impact of past cyberloafing on interactional justice is significant at the 0.10 level, but not at the 0.05 level (parameter estimate = -0.09,  $p < 0.010$ , two-tailed). Thus, this hypothesis was marginally supported (H2 marginally supported). Finally, we predicted that organizational commitment would be positively associated with interactional justice. Figure 2 shows that organizational commitment has a strong positive impact on interactional justice (parameter estimate = 0.33,  $p < 0.001$ , two-tailed; H3 supported).

#### 3.5.2 Negative emotions

Two hypotheses related to the formation of negative affective reactions. In particular, we argued that cyberloafing before implementation of technology to prevent it would increase negative affective reactions after the implementation of such technology. The results indicate that interactional justice and negative affective reactions are negatively related. Indeed, interactional justice was found to have a negative impact on negative affective reactions (parameter estimate = -0.40,  $p < 0.001$ , two-tailed; H4 supported). We also found that the relationship between past cyberloafing and negative affective reactions is positive and significant (parameter estimate = 0.33,  $p < 0.001$ , two-tailed), which supports the hypothesis (H5 supported).

#### 3.5.3 Perceived fairness

We previously predicted that negative affective reactions would reduce the level of perceived fairness. Consistent with this hypothesis, we found that negative affective reactions have a negative relationship with perceived fairness (parameter estimate = -0.21,  $p < 0.001$ , two-tailed; H6 supported). We also hypothesized that perceived fairness was a function of interactional justice and negative affective reactions. In particular, our hypothesis suggest that interactional justice would positively affect perceived



**Fig. 2** Results. Bold paths were hypothesized. N = 552; \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$ . CNTX context, AGE age, GEN gender, ATT attitudes, SN subjective norm, PBC perceived behavioral control, PCL

past cyberloafing, OC organizational commitment, IJ interactional justice, NE negative emotions, PF perceived fairness, CLI cyberloafing intention, LOYI loyalty intention

fairness. As indicated in Fig. 2, interactional justice relates positively with perceived fairness (parameter estimate = 0.76,  $p < 0.001$ , two-tailed; H7 supported). Besides, we proposed that negative affective reactions would strengthen the relationship between interactional justice and perceived fairness. Our results show that the interaction effect between interactional justice and negative affective reactions on perceived fairness is positive and significant (parameter estimate = 0.07,  $p < 0.01$ , two-tailed). Thus, this moderation hypothesis is supported (H8 supported).

### 3.5.4 Cyberloafing intention

We argued earlier that fairness perceptions would positively affect cyberloafing following the implementation of the cyberloafing technology. The direct effect of perceived fairness on cyberloafing after technological intervention is found to be positive and significant (parameter estimate = 0.13,  $p < 0.05$ , two-tailed), which supports our hypothesis (H9 supported).

### 3.5.5 Loyalty intention

Finally, we examined the hypothesis predicting that perceived fairness would relate positively to loyalty after implementing the technology. The results indicate that

overall fairness indeed have a positive impact on loyalty after the implementation of cyberloafing technology (parameter estimate = 0.32,  $p < 0.001$ , two-tailed). Hence, this final hypothesis is also supported (H10 supported).

## 4 Discussion

Our goal in this paper was to study the effect that implementation of new anti-cyberloafing technologies have on employees' cyberloafing intentions and loyalty. We proposed a justice-based model that captures how a technological intervention affects individuals' psychological reactions and that relates employees' past cyberloafing and organizational commitment, respectively, to their cyberloafing and loyalty after technological intervention. Our findings suggest that cyberloafing technological intervention, although associated with perceptions of unfairness, can curb cyberloafing albeit at the expense of employee loyalty. Meanwhile, contrary to prior findings, we find that fairness perceptions of technological interventions, although reinforcing employee loyalty, are ineffective at curbing cyberloafing. These findings are especially enlightening in that they contradict the intuition that perceived fairness should encourage employees to curb their misuse of IT out of appreciation for the fairness displayed by management.

#### 4.1 Theoretical contributions

In an attempt to understand cyberloafing behavior, prior research has focused on identifying significant predictors of such undesirable behavior as low levels of perceived organizational justice [41], lack of organizational commitment [20], work boredom and lack of involvement [21, 38], lax organizational culture [20, 64], and peers' cyberloafing [41, 68, 81]. Unlike these past studies that focused on the determinants of cyberloafing, our paper is unique in that it examines how individuals' cognitive and emotional reactions to technological interventions determine their future cyberloafing and loyalty intentions. Our paper draws upon justice theories to reveal a causal mechanism through which cognitive and affective components interact to eventually form an overall judgment of the fairness of newly-implemented anti-cyberloafing technologies. Although interactional justice is already considered as an important factor in IS research, little is known about the difference between immediate, specific evaluations (i.e., interactional justice) and an overall evaluation of the justice surrounding cyberloafing in the workplace. This study is one of the first to show that interactional justice, as an immediate and specific evaluation, eventually translates into a more overarching concept like perceived fairness regarding the implementation of technology to prevent cyberloafing.

Additionally, our study reveals new insights into the role of affective reactions in the context of cyberloafing prevention. Much research on cyberloafing is focused simply on cognitive judgments without considering the important role of affective reactions in evaluating technological interventions that are perceived as privacy-threatening. Our findings indicate that negative affective reactions not only determine perceived fairness but also moderate the effect of interactional justice on perceived fairness. Specifically, our results reveal that the relationship between specific and overall judgments can be strengthened as a result of negative affective reactions, making interactional justice even more important for perceived fairness. Taken together, our study pushes the boundary of the justice framework by clarifying complex relationships between specific justice perceptions (i.e., interactional justice), affective reactions (i.e., negative emotions), and a psychological synthesis of the beliefs and feelings toward a privacy-threatening technology.

Much research shows that organizational interventions influence individuals' behavior within highly experimental settings. However, experimental studies have limitations in studying organizational behaviors such as cyberloafing and loyalty because those behavioral outcomes are largely shaped by factors such as cyberloafing before the technological intervention to diminish it, and organizational

commitment. In this sense, this study contributes to the literature by showing theoretically and empirically that past cyberloafing behavior can translate into negative affective reactions when such technology is implemented. Our results reveal that employees tend to assess the justice of organizational changes from the viewpoint of their recent individual reference points. Past cyberloafers feel that new cyberloafing technology single them out and specifically targets them. Thus, for former cyberloafers, a new cyberloafing technology stirs an amalgamation of negative feelings of induced system restrictiveness, and desperation that can translate into revolt and anger in the workplace, negatively impacting loyalty and potentially increasing turnover. We found that organizational commitment positively affects interactional justice, which suggests that committed employees are more receptive of new cyberloafing policies and more likely to accept such technology. These findings imply that although organizational measures are important in changing employees' perceptions, it is essential to consider organizational commitment in assessing how they react to new policies embedded in technology solutions.

Finally, although some research has suggested that perceived fairness is critical to aligning the interests of employees with the success of their firms, other research has discovered that deterrence and punishment are the only effective means to correct employees' misbehavior [36, 55, 78]. Taken separately, these two results seem contradictory because punishment carries the stigma of unfairness [25, 78]. It was found that zero tolerance, progressive discipline, and appeal processes are related to higher perceptions of policy fairness while periodic monitoring is related to less cyberloafing [25]. In this paper, we have consolidated the two streams of research by developing a justice-based theoretical model that shows the repercussions of perceived fairness on cognitive and affective outcomes explaining cyberloafing loyalty after implementing the technology. Unlike in prior literature in which perceptions of fairness were shown to be effective in limiting employees' deviant behavior, our results show that such fairness can actually have the unintended consequences of sustaining cyberloafing. Our findings imply that organizational policies and technological interventions that create perceptions of unfairness, although decreasing employee loyalty and thereby increasing the risk of employee turnover [82], can be effective at curbing cyberloafing. The perceived risk of not only getting fired but also, and more importantly, of having to carry the stigma of being a cyberloafers seems to work as a deterrent to curb future cyberloafing. As time goes on, employees who curbed their cyberloafing may readjust their perceptions and expectations of fairness, which in turn can boost their loyalty toward the organization, and hence involving

and guiding the employees during the implementation of this technology in the workplace can help alleviate negative affective reactions. Thus, another major contribution of this paper lies in revealing this dual nature of perceived fairness in the context of cyberloafing. On the one hand, a gentle approach to curbing cyberloafing helps to boost subjective fairness perceptions and eventually maintain workers' loyalty to the organization. On the other hand, such an approach alone without proper technological intervention will not be instrumental in addressing the cyberloafing problem in the organization. Our proposed model yields a theoretical explanation for paradoxical phenomena in which the organizational policies that workers perceive as fair are not necessarily effective in curbing cyberloafing even though perceived fairness is conducive to the formation of loyalty.

#### 4.2 Managerial implications

The results of this study can help motivate managers to view anti-cyberloafing technological interventions as more than just a statement of expected employee behavior. Employees' reaction to a new cyberloafing policy embedded in technology is mediated by a complex set of appraisals and heuristics. Thus, in crafting a policy, managers must consider both the implications of rational justice appraisals as well as affective heuristics. But, importantly, an effective cyberloafing policy must serve as an instrument that transforms the fairness perceptions of employees.

Our results show that after a policy on cyberloafing has been introduced, the sense of (un)fairness that employees ultimately feel can influence their future cyberloafing intentions and loyalty. In this sense, when management introduces a cyberloafing policy, proper care should be exercised (e.g., through training, proper change management, and organizational communication) to manage factors such as negative emotions and interactional justice that influence perceived fairness. Because perceived fairness comes from processes of cognitive appraisal and affective heuristic responses, it has equally complex repercussions. We saw that implementing such policies and technology, although perceived as unfair, can curb future cyberloafing but this comes at the cost of adversely affecting loyalty. Therefore, a cyberloafing policy must be part of a larger effort that simultaneously seeks to boost long-term employee commitment and create a dialogue about organizational engagement.

Nonetheless, the sense of unfairness brought about by cyberloafing policies can serve as an effective instrument for short-term gains against cyberloafing. In this respect, the tone of a policy directly conveys displeasure from management and sets expectations for future behavior. For the most chronic offenders, a cyberloafing policy allows

managers to achieve immediate course correction if the situation warrants it. The antecedents of perceived fairness also suggest ways in which managers can fine-tune their policy to achieve their desired results. In particular, if the goal of managers is to reduce turnover, they could provide adequate explanations and treat employees fairly to strengthen their loyalty. However, if cyberloafing behavior occurs rather frequently and on a continual basis during the workday and managers feel that it is imperative to quickly remedy the problem, then they can impose mandatory measures that would drive employees to quickly curb their cyberloafing.

Managers should also consider the commitment of their employees when implementing new anti-cyberloafing technological measures. Before employees can appraise the fairness of such measures, they evaluate the interactional justice associated with the delivery of such measures. The quality of information content and the quality of interpersonal delivery both determine feelings of fairness and anger. But the complexity of processing a security policy leaves employees resorting to their prior sense of commitment to appraise the quality of justice [14, 59]. Thus, even a harsh enforcement of policy and restrictive technology will have a relatively muted effect on committed employees. On the other hand, less committed employees will tend to have an adverse reaction to a cyberloafing policy, regardless of the policy's level of enforcement. Thus, managers might be free to pick the most effective policy they want, safe in the knowledge that it will serve as a warning to uncommitted employees and that its relatively minor disruptive effect on committed employees can be managed by other means. Employees' final appraisal of interactional justice will strongly influence their final perceptions of fairness, although some employees may respond with anger.

Altogether, managers should craft their anti-cyberloafing interventions knowing that current employees will process these instruments through the prism of perceived fairness. Counterintuitively, a level of perceived unfairness helps induce changes in behavior and break habitual cyberloafing. Chronic offenders will have a markedly larger affective response, but committed and nonoffending employees will respond relatively less severely to the enforcement. Nonetheless, we reemphasize that the consequent damage to loyalty must be addressed through a broader dialogue.

#### 4.3 Limitations and future research directions

Our model investigates the relationships amongst perceived interactional justice, negative emotions, and perceived fairness. Interactional justice and anger predict most of the variances of perceived fairness, which means they

are key factors in any investigation of policy. However, the antecedents of interactional justice and negative emotions explain less than a third of these two factors. No full understanding has yet been reached on what triggers the decision-making process of employees and what factors influence appraisal and emotion. Thus, although our model introduces the important pathways linking justice, anger, and fairness, a story remains to be told about how this process begins.

Our study also looked at cyberloafing and security policies with an eye on enforcement. Consequently, we chose two scenarios of policy enforcement that represent alternative levels of intrusiveness and control by management. Nonetheless, we do not discount other ways of limiting cyberloafing. For example, management could choose such extremes as not having a central policy or having a mandatory technical policy that cuts access to outside network resources. These other means of limiting cyberloafing could entail policing by peers [68, 81], technical staff, or automated means. Absolving management from the responsibility for enforcement or limiting opportunities to cyberloaf are also strategies that bear investigation, although they are outside the scope of this study.

Along similar lines, our choice of policy strategies created large variances in perceived unfairness, which drove future intentions. Our study simply recognizes that managerial interventions primarily influence the behavior of employees because of perceived unfairness. But instead of introducing an enforcement policy, while beyond the results of this study, future research should study how organizations might seek more holistic ways of curbing the misuse of IT resources by engendering a greater sense of responsibility and citizenship, and performance metrics that are outcome-based rather than process based. Hence, if employees do their job well, the organization will not worry if the employees cyberloaf periodically to break the monotony of their work or to learn something that may have positive long-term implications for their work to enhance loyalty.

We must also recognize that several methodological choices made in this study may limit how our results are interpreted. This study collected cross-sectional data without eventual outcome behaviors. Thus, we cannot make a definitive link between policy choices and actual reductions in cyberloafing, or analyze how the process of appraisal, emotional response, and fairness evolves over time. This study is focused on the immediate reaction of employees to a cyberloafing policy.

The limitations presented above suggest several promising directions for future research on cognitive appraisals of cyberloafing policy. We believe that follow-up studies could look at the possible antecedents of negative emotions and interactional justice, conduct

longitudinal studies of employee perceptions, and investigate alternative strategies to limiting or dissuading cyberloafing. However, the overall appraisal process uncovered in this study also suggests fundamentally new areas of investigation into the psychology of cyberloafing and security.

We must also gain a better understanding of the contrasting perspectives on cyberloafing between management and employees. Managers employ cyberloafing policies to achieve productivity gains. But we found that employees respond to such policies with negative feelings and perceptions of unfairness, which belie a sense of loss. Recently, researchers have begun to realize that consumers perceive security measures as loss prevention, not as the securing of future gains [4, 31, 64]. People with a loss perspective are much more likely to favor risky options [31]. Consequently, security experts now suggest that the loss perspective predisposes people to not employ security tools and to avoid security measures [31, 56, 64]. Although our study suggests ways in which managers can curb cyberloafing by employing the inevitable responses of anger and unfairness, future research must also investigate how to reframe security interventions, such as new cyberloafing policies, as gainful and favorable solutions for employees.

#### 4.4 Conclusions

We developed a model to study cyberloafing and technological intervention and tested the model using a combination of field surveys utilizing a set of scenarios. Our results reveal that, within the context of cyberloafing prevention, past cyberloafing, context, and organizational commitment are three important considerations that should be accounted for to accurately assess interactional justice, negative affective reactions, and perceived fairness; we found these factors to determine behavioral outcomes. What is important, and contrary to common belief, is that organizational measures that engender unfairness perceptions in employees are surprisingly capable of effectively curtailing cyberloafing, albeit at the expense of employee loyalty. These results, we hope, will help organizations better craft effective anti-cyberloafing technological interventions that preserve the loyalty of committed employees to maintain their talent pool.

#### Appendix: Measures and scenarios\*

##### Part A

##### Attitudes toward cyberloafing (ATT)

- Using the Internet at work for non-work-related purposes is a wise idea.



- I like the idea of using the Internet at work for non-work-related purposes.
- Using the Internet at work for non-work-related purposes is pleasant.

#### Subjective norm (SN)

- People who influence my behavior think that it is fine for me to use the Internet at work for non-work-related purposes occasionally.
- People who are important to me think that it is fine for me to use the Internet at work for non-work-related purposes once in a while.

#### Perceived behavioral control (PBC)

- I can use the Internet at work for non-work-related purposes whenever I want.
- It is easy for me to use the Internet at work for non-work-related purposes.
- I have control over using the Internet at work for non-work-related purposes.

#### Past cyberloafing (PCL)

- On average, how frequently have you used the Internet at work for non-work-related purposes over the past month? (1 = less than once a week; 2 = a few times a week; 3 = about one a day; 4 = a few times a day; 5 = once an hour; 6 = several times an hour).
- I frequently use the Internet at work for non-work related purposes on a typical day.

#### Organizational commitment (OC)

- I am proud to be working for this organization.
- I find that my values and those of the organization are very similar.
- I feel loyal to this organization.
- I am willing to work harder than I have to in order to help this organization succeed.

#### Part B

##### Scenarios (CNTX)

Your management team announces that a new information system will be implemented to keep track of your use of the Internet in the organization (e.g., emails, social networking services, online news, software downloads, and financial transactions).

- They indicate that the new system will generate a weekly report on the websites you visited, and the management team will review the report. [CNTX = 1]
- They indicate that the new system will generate a weekly report on the websites you visited, but the report will be sent to you only. The report will NOT be sent to anyone else. [CNTX = 2].

#### Interactional justice (IJ)

- In the scenario described previously, the management team treats me in a kindly manner.
- In the scenario described previously, the management team shows concern for my rights as an employee.
- In the scenario described previously, the management team behaves in a way that fosters trust on my part.

#### Negative emotions (NE)

When you read the previous announcement by the organization, to what extent did you experience the following feelings? (1 = not at all to 7 = to a great extent).

- Furious
- Irritated
- Angry

#### Perceived fairness (PF)

- The management team is fair in this plan.
- This new plan is reasonable.
- I feel I am treated fairly by the management team.

#### Cyberloafing intention (CLI)

- I predict that I would use the Internet at work for non-work-related purposes.
- I intend to use the Internet at work for non-work-related purposes.
- I plan to use the Internet at work for non-work-related purposes.

#### Loyalty intention (LOYI)

- I will defend the organization when outsiders criticize it.
- I will encourage friends and family to utilize the organization's products and services.
- I will stand up to protect the reputation of the organization.

#### Part C

##### Control variables

- Age: (Years old)
- Gender: (1 = male; 2 = female)

Note: \* Unless otherwise indicated, the anchors for all items were 1 = strongly disagree to 7 = strongly agree.

## References

1. Ajzen I (1985) From intentions to actions: a theory of planned behavior. In: Kuhl J, Beckman J (eds) Action control: from cognition to behavior. Springer, New York, pp 11–39

2. Anandarajan M (2002) Profiling web usage in the workplace: a behavior-based artificial intelligence approach. *J Manag Inf Syst* 19(1):243–266
3. Anandarajan M, Simmers C (2005) Developing human capital through personal web use in the workplace: mapping employee perceptions. *Commun Assoc Inf Syst* 15:776–791
4. Anderson C, Agarwal R (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Q* 34(3):613–643
5. Askew K, Buckner J, Taing M, Ilie A, Bauer J, Coovert M (2014) Explaining cyberloafing: the role of the theory of planned behavior. *Comput Hum Behav* 36:510–519
6. Bagozzi R, Yi Y (1988) On the evaluation of structural equation models. *J Acad Mark Sci* 16(1):74–94
7. Bearden W, Netemeyer R, Mobley M (1993) Handbook of marketing scales: multi-item measures for marketing and consumer behavior research. Sage Publications, Newbury Park
8. Bies R (2001) Interactional (in) justice: the sacred and the profane. In: Greenberg J, Cropanzano R (eds) *Advances in organizational justice*. Stanford University Press, Stanford, pp 89–118
9. Bonifield C, Cole C (2007) Affective responses to service failure: anger, regret, and retaliatory versus conciliatory responses. *Mark Lett* 18(1–2):85–99
10. Campbell MC (2007) “Says who?!” How the source of price information and affect influence perceived price (un) fairness. *J Mark Res* 44(2):261–271
11. Cheng L, Li W, Zhai Q, Smyth R (2014) Understanding personal use of the Internet at work: an integrated model of neutralization techniques and general deterrence theory. *Comput Hum Behav* 38:220–228
12. Chin W, Gopal A, Salisbury W (1997) Advancing the theory of adaptive structuration: the development of a scale to measure faithfulness of appropriation. *Inf Syst Res* 8(4):342–367
13. Colquitt J, Rodell J (2015) Measuring justice and fairness. *Oxford handbook of justice in the workplace*, 187–202
14. Colquitt J, Scott B, Rodell J, Long D, Zapata C, Conlon D, Wesson M (2013) Justice at the millennium, a decade later: a meta-analytic test of social exchange and affect-based perspectives. *J Appl Psychol* 98(2):199
15. Culnan M, Bies R (2003) Consumer privacy: balancing economic and justice considerations. *J Soc Issues* 59(2):323–342
16. Farh J, Earley P, Lin S (1997) Impetus for action: a cultural analysis of justice and organizational citizenship behavior in Chinese society. *Adm Sci Q* 42(3):421–444
17. Finkel NJ (2001) Not fair! The typology of commonsense unfairness. American Psychological Association, Washington, DC
18. Folger R, Skarlicki DP (1999) Unfairness and resistance to change: hardship as mistreatment. *J Org Change Manag* 12(1):35–50
19. Fornell C, Larcker D (1981) Evaluating structural equation models with unobservable variables and measurement error. *J Mark Res* 18(1):39–50
20. Garrett R, Danziger J (2008) Disaffection or expected outcomes: understanding personal Internet use during work. *J Comput Med Commun* 13(4):937–958
21. Gefen D, Straub D, Boudreau M (2000) Structural equation modeling and regression: guidelines for research practice. *Commun Assoc Inf Syst* 4(7):1–77
22. Guo K, Yuan Y, Archer N, Connelly C (2011) Understanding nonmalicious security violations in the workplace: a composite behavior model. *J Manag Inf Syst* 28(2):203–236
23. Haidt J (2001) The emotional dog and its rational tail: a social intuitionist approach to moral judgment. *Psychol Rev* 108:814–834
24. Hair JF Jr, Anderson RE, Tatham RL, Black WC (1995) *Multivariate data analysis*, 3rd edn. Macmillan, New York
25. Henle C, Kohut G, Booth R (2009) Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: an empirical test of justice theory. *Comput Hum Behav* 25(4):902–910
26. Herscovitch L, Meyer JP (2002) Commitment to organizational change: extension of a three-component model. *J Appl Psychol* 87(3):474–487
27. Hu L, Bentler P (1999) Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. *Struct Equ Model A Multidiscip J* 6(1):1–55
28. Iverson RD (1996) Employee acceptance of organizational change: the role of organizational commitment. *Int J Hum Resour Manag* 7(1):122–149
29. Jöreskog K, Sörbom D (1996) LISREL8: user’s reference guide. Scientific Software International, Chicago
30. Khansa L, Kuem J, Siponen M, Kim S (2017) To Cyberloaf or not to cyberloaf: the impact of the announcement of formal organizational controls. *J Manag Inf Syst* 34(1):141–176
31. Khansa L, Liginlal D (2009) Valuing the flexibility of investing in information security process innovations. *Eur J Oper Res* 192(1):216–235
32. Khansa L, Xiao M, Liginlal D, Kim S (2015) Understanding members’ active participation in online question-and-answer communities: a theory and empirical analysis. *J Manag Inf Syst* 32(2):162–203
33. Kim S, Malhotra N, Narasimhan S (2005) Two competing perspectives on automatic use: a theoretical and empirical comparison. *Inf Syst Res* 16(4):418–432
34. Kim S, Son J (2009) Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the context of online services. *MIS Q* 33(1):49–70
35. Kumar N, Scheer L, Steenkamp J (1995) The effects of supplier fairness on vulnerable resellers. *J Mark Res* 32(1):54–65
36. Lee S, Lee S, Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Inf Manag* 41(6):707–718
37. Li H, Sarathy R, Zhang J, Luo X (2014) Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Inf Syst J* 24(6):479–502
38. Liberman B, Seidman G, McKenna K, Buffardi L (2011) Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Comput Hum Behav* 27(6):2192–2199
39. Lim V (2002) The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *J Organ Behav* 23(5):675–694
40. Lim V, Teo T (2005) Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: an exploratory study. *Inf Manag* 42:1081–1093
41. Lim V, Teo T, Loo G (2002) How do I loaf here? Let me count the ways. *Commun ACM* 45(1):66–70
42. Lindell M, Whitney D (2001) Accounting for common method variance in cross-sectional research designs. *J Appl Psychol* 86(1):114–121
43. Malhotra N, Kim S, Patil A (2006) Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research. *Manag Sci* 52(12):1865–1883
44. Marsden P, Kalleberg A, Cook C (1993) Gender differences in organizational commitment: influences of work positions and family roles. *Work Occup* 20(3):368–390
45. Maruping L, Magni M (2012) What’s the weather like? The effect of team learning climate, empowerment climate, and gender on individuals’ technology exploration and use. *J Manag Inf Syst* 29(1):79–113

46. Mathews BP, Shepherd JL (2002) Dimensionality of Cook and Wall's (1980) British Organizational Commitment scale. *J Occup Organ Psychol* 75:369–375
47. Moody G, Siponen M (2013) Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Inf Manag* 50(6):322–335
48. Moorman R, Blakely G, Niehoff B (1998) Does perceived organizational support mediate the relationship between procedural justice and organizational citizenship behavior? *Acad Manag J* 41(3):351–357
49. Mowday RT, Steers R, Porter LW (1979) The measurement of organizational commitment. *J Vocat Behav* 14(2):224–247
50. O'Guinn T, Faber R (1989) Compulsive buying: a phenomenological exploration. *J Consum Res* 16(2):147–157
51. Olivier RL (1999) Whence consumer loyalty? *J Mark* 63:33–44
52. Posey C, Bennett R, Roberts T, Lowry P (2011) When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *J Inf Syst Sec* 7(1):24–47
53. Rahim M, Magner N, Shapiro D (2000) Do justice perceptions influence styles of handling conflict with supervisors? What justice perceptions, precisely? *Int J Confl Manag* 11(1):9–31
54. Robinson S, Morrison E (2000) The development of psychological contract breach and violation: a longitudinal study. *J Organ Behav* 21(7):855
55. Schmidt T, Houston M, Bettencourt L, Boughton P (2003) The impact of voice and justification on students' perceptions of professors' fairness. *J Mark Educ* 25(2):177–186
56. Schneier B (2008) How the human brain buys security. *IEEE Sec Priv* 6(4):80
57. Schoefer K, Ennew C (2005) The impact of perceived justice on consumers' emotional responses to service complaint experiences. *J Serv Mark* 19(5):261–270
58. Schwartz B (2000) Self-determination: the tyranny of freedom. *Am Psychol* 55(1):79–88
59. Seifert M, Brockner J, Bianchi E, Moon H (2016) How workplace fairness affects employee commitment. *MIT Sloan Manag Rev* 57(2):15
60. Seo M, Barrett L, Bartunek J (2004) The role of affective experience in work motivation. *Acad Manag Rev* 29(3):423–439
61. Siponen M, Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Q* 34(3):487–502
62. Son J, Kim S (2008) Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS Q* 32(3):503–529
63. Son J, Park J (2016) Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: its determinants and interaction with privacy concerns. *Int J Inf Manag* 36:309–321
64. Tang M, Zhang T (2016) The impacts of organizational culture on information security culture: a case study. *Inf Technol Manag* 17(2):179–186
65. Taylor S, Todd P (1995) Understanding information technology usage: a test of competing models. *Inf Syst Res* 6(2):144–176
66. Terry D, Oleary J (1995) The theory of planned behavior: the effects of perceived behavioral-control and self-efficacy. *Br J Soc Psychol* 34:199–220
67. Ugrin J, Pearson J (2013) The effects of sanctions and stigmas on cyberloafing. *Comput Hum Beh* 29:812–820
68. Umphress E, Labianca G, Brass D, Kass E, Scholten L (2003) The role of instrumental and expressive social ties in employees' perceptions of organizational justice. *Organ Sci* 14(6):738–753
69. Vance A, Lowry P, Eggett D (2013) Using accountability to reduce access policy violations in information systems. *J Manag Inf Syst* 29(4):263–289
70. Vance A, Siponen M (2012) IS security policy violations: a rational choice perspective. *J Organ End User Comput* 24(1):21–41
71. Venkatesh V, Davis F (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. *Manag Sci* 46(2):186–204
72. Wang J, Tian J, Shen Z (2013) The effects and moderators of cyber-loafing controls: an empirical study of Chinese public servants. *Inf Technol Manag* 14:269–282
73. Weber PS, Weber JE (2001) Changes in employee perceptions during organizational change. *Leadersh Organ Dev J* 22(6):291–300
74. Weckert J (2005) *Electronic monitoring in the workplace: controversies and solutions*. Idea Group Publishing, Hershey
75. Williams LJ, Anderson SE (1991) Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *J Manag* 17:601–617
76. Willison R, Warkentin M (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Q* 37(1):1–20
77. Xia L, Monroe KB, Cox JL (2004) The price is unfair! A conceptual framework of price fairness perceptions. *J Mark* 68(4):1–15
78. Xue Y, Liang H, Wu L (2011) Punishment, justice, and compliance in mandatory IT settings. *Inf Syst Res* 22(2):400–414
79. Yoon J, Thye SR (2002) A dual process model of organizational commitment. *Work Occup* 29(1):97–124
80. Zangaro GA (2001) Organizational commitment: a concept analysis. *Nurs Forum* 36(2):14–22
81. Zhang D, Lowry P, Zhou L, Fu X (2007) The impact of individualism-collectivism, social presence, and group diversity on group decision making under majority influence. *J Manag Inf Syst* 23(4):53–80
82. Zhao H, Wayne S, Glibkowski B, Bravo J (2007) The impact of psychological contract breach on work related outcomes: a metaanalysis. *Pers Psychol* 60(3):647–680