I'LL BE WATCHING YOU: AI SURVEILLANCE TECHNOLOGIES AND PRIVACY INVASION

A Thesis

Presented to the Faculty of the Graduate School

of Cornell University

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

by

Rachel Jean Schlund

May 2020

ABSTRACT

Within the last few decades, we have witnessed the dramatic rise in the use of AI surveillance technologies in organizations. In this paper, we answer calls from management scholars to investigate the impact of this new aspect of organizational control on manager-worker dynamics. Focusing on employees' perceptions of privacy invasion, we investigate in four experimental studies whether these differ when the observer is a form of AI technology instead of a human. We demonstrate that employees perceive their privacy is invaded to a greater extent when AI surveillance technologies monitor them as opposed to human managers (Studies 1-4). We further assess downstream consequences of perceived privacy invasion (Studies 1-2), explore mechanisms that explain the relationship between monitoring form (AI surveillance technologies vs. human managers) and perceived privacy invasion (Study 3), and investigate ways to attenuate the effect (Study 4). Throughout these studies, we extend prior theory to provide insight into the implications of the increasing use of AI surveillance technologies in organizations.

BIOGRAPHICAL SKETCH

Rachel Schlund was raised in Chico, California. She received a BA in Psychology from University of California, Santa Cruz and graduated s*umma cum laude* with highest honors in the major in 2018. She started her PhD in Organizational Behavior at Cornell University in 2018.

In loving memory of my mother, Dr. Rebekah Wold.

ACKNOWLEDGMENTS

I wish to thank, first and foremost, my advisor, Dr. Emily Zitek of Organizational Behavior at Cornell University. It is with immense gratitude that I acknowledge her unwavering support and guidance. Her belief in my ability as a researcher continues to instill the confidence and motivation to pursue my research interests, while her knowledge and advice remain invaluable for my academic development and ability to conduct rigorous research. I would also like to thank my advisors Dr. Vanessa Bohns of Organizational Behavior at Cornell University and Dr. Pamela Tolbert of Organizational Behavior at Cornell University. I am honored to acknowledge their advice and encouragement as they continue to be integral to my academic and personal development. This thesis would not have been possible without them.

I would also like to further extend my gratitude to my colleges in ExPO Lab (Cornell ILR/ Johnson) as their feedback has been extremely helpful for the development and advancement of this project. Finally, I would also like to especially thank my father, Dr. James Schlund, my friends, and my family for their unequivocal support throughout, as always, for which I am extremely grateful.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I'll Be Watching You: AI Surveillance Technologies and Privacy Invasion

The last few decades have born witness to the dramatic rise in the use of artificial intelligence (AI) surveillance technologies in organizations, vastly reshaping managerial oversight and even organizational control systems at large (Kellogg, Valentine, & Christin, 2020). When Fredrick Taylor (1911) originally proposed the use of scientific management, oversight by management typically involved the use of human managers who tracked production and return on investments, and walked around the factory floor to intermittently observe employees (Bernstein, 2017; Dalton, 1959). However, in today's workplace, management is equipped with technology that allows for the monitoring of employees in new and different ways. To illustrate, a survey conducted by the American Management Association (2007) revealed that 66% of responding organizations monitor employees' web-browsers, 45% monitor employees' keystrokes, and 43% monitor employees' emails. Further, 55% of responding organizations said that they surveil employees via video recording technology—a 20% increase from 2001.

Importantly, it is now possible to equip these forms of monitoring and surveillance technologies with AI. That is, unlike previous surveillance technologies, such as simple CCTV cameras, AI surveillance technologies are equipped with artificial intelligence or "…computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages" (Jewell & Abate, 2010, p.91). These AI surveillance technologies enable management to replace human managers and simple surveillance technologies, both of which are constrained by human judgment,

attention, and decision-making that make them far more fallible than AI surveillance technologies, which can continuously watch, analyze, and make decisions regarding employees' behavior. For example, AI can automatically track and analyze employees' facial expressions, tone of voice, and written communication line-by-line such as employees' emails, instant messages, and their social media engagement (Ball, 2010; Ball, Haggerty, & Lyon, 2012; Bernstein, 2014, 2017; Levinson, 2009; Peck, 2013; Smith-Butler, 2009). Moreover, some organizations are implementing invasive AI surveillance technologies, such as requiring employees to wear tracking devices equipped with GPS, biosensors to record and analyze employees' biometric data, and accelerometers that track employees' movement and activity (Bernstein, 2017; Kantor & Streitfeld, 2015; Rawlinson, 2013; Frost & Sullivan, 2017).

The increasing adoption of AI surveillance technologies in organizations has ignited a growing body of research investigating its effects in organizations (e.g., for a review see Alge & Hansen, 2014; Ball et al., 2012; Ball, 2010). As a result, research on privacy invasion has been brought to the forefront of management studies (Acquisti, Brandimarte, & Loewenstein, 2015; Bernstein, 2017; Bhave, Teo, & Dalai, 2020). Past research on non-AI forms of monitoring have found that when organizations administer control over their employees by monitoring them, employees may feel that their privacy is being invaded, which can have unintended negative downstream consequences for organizations. For example, when employees feel that their privacy is being invaded, it can decrease their trust (Miller & Weckert, 2000), reduce inter-organizational communication (Botan, 1996; Holton & Fuller, 2008), and reduce employees' productivity and compliance with rules and procedures (Alge et al.,

2010; Zweig & Scott, 2007). Moreover, actually increasing the level of privacy in an organization has been linked to boosts in performance (Bernstein, 2012).

Although previous research has investigated aspects of workplace monitoring and employees' perceptions of privacy invasion (e.g., Alge et al., 2010; Allen, Walker, Coopman, & Hart, 2007; McNall & Roch, 2009; McNall & Stanton, 2011; Zweig & Webster, 2002), research has yet to investigate the effects of AI surveillance technologies on employees' perceptions of privacy invasion, which is important as the use of AI surveillance technologies enable management to ubiquitously observe employees, while also removing human discretion, which is unprecedented: carrying the potential to reshape organizational control systems (Kellogg et al., 2020). As a result, organizations are at risk for unintentionally producing negative downstream consequences when implementing AI surveillance technologies, which is increasingly occurring throughout modern labor markets.

Thus, researching the relationship between AI surveillance technologies and the factors that lead to perceptions of privacy invasion in the workplace is of both practical and theoretical importance for management scholars (Bernstein, 2017; Bhave et al., 2020; Kellogg et al., 2020). The current research aims to extend prior theory to investigate the effect of monitoring form, specifically monitoring via human management and monitoring via AI surveillance technologies, on employees' perception of privacy invasion. In doing so, we answer calls from management scholars to investigate the impact of this new aspect of organizational control on manager-worker dynamics (Bernstein, 2017; Bhave et al., 2020; Kellogg et al., 2020). Across four experimental studies, we examine the relationship between employees'

perceptions of privacy invasion and monitoring form, specifically focusing on monitoring via AI surveillance technologies versus monitoring by a human manager.

The Effect of AI Surveillance Technologies on Employees' Perception of Privacy Invasion

The study of privacy and the experience of privacy invasion has been a topic of interest for over 60 years (e.g., Goffman, 1959; Merton, 1957; Schwartz, 1968), and has recently gained momentum due to the increasing use of AI surveillance technologies (Acquisti et al., 2015; Ball et al., 2012; Bhave et al., 2020; Kellogg et al., 2020). Although the definition of privacy remains widely contested (Bernstein, 2017; Bhave et al., 2020), most scholars agree that privacy entails the capacity of an individual to control their information and interaction with others in the environment (Bhave et al., 2020; Stone & Stone, 1990). However, an individual's perception of privacy invasion is more nuanced than privacy *per se*. Perceived privacy invasion does not solely account for an individual's *actual* capacity to control their information and interaction with others in the environment, but their *perceived* capacity to do so (Bhave et al., 2020). Therefore, scholars have theorized that individuals possess a "privacy calculus"—a cost-benefit analysis of the potential risks and benefits of providing access to their information that accounts for the *extent* to which one perceives that their privacy is invaded (Bhave et al., 2020; Culnan & Armstrong, 1999; Laufer & Wolfe, 1977). Thus, when individuals perceive the risks of relinquishing control over their information are greater than the perceived benefits of doing so, individuals will perceive that their privacy is invaded to a greater extent.

Applying the privacy calculus model to the context of monitoring in organizations (Bhave et al., 2020; Culnan & Armstrong, 1999; Laufer & Wolfe, 1977), we believe employees are more likely to think that their privacy is invaded when AI surveillance technologies monitor them as opposed to human managers for the following reason: employees will think that they face greater risks (i.e., negative consequences) when monitored by AI surveillance technologies rather than human managers because AI surveillance technologies can engage in ubiquitous monitoring and cannot grant exceptions for justifiable mistakes or drops in performance as they remove human discretion. For example, human managers lack the ability to monitor employees continuously. In addition, human managers lack the ability to comprehensively and infallibly review all of the non-AI technology enabled surveillance systems in an organization. However, AI surveillance technologies can engage in ubiquitous and infallible monitoring. AI surveillance technology does not need to take breaks; it does not get distracted; it does not become tired: it can always engage in surveillance. Since AI surveillance technologies have the ability to engage in surveillance ubiquitously, employees may perceive they have a higher risk of facing negative consequences because they are more likely to be caught and reprimanded for performing poorly or making mistakes. Conversely, the inability of human management to continuously observe employees may cause employees to feel less concerned about facing negative consequences because human managers are less likely to catch and reprimand employees every time they perform poorly or make a mistake—indeed, even the most ethical and motivated employees can have off days.

Further, the use of AI surveillance technologies leads to what Kellogg et al. (2020) termed the "disintermediation of managers"—the replacement of managerial oversight with algorithmic oversight. That is, AI is able replace human supervision since it can perform tasks that normally require human intelligence— AI is able to continuously watch, analyze, and make decisions regarding employees' behavior without direct supervision by human managers. In doing so, organizations significantly reduce the role of human discretion that has traditionally encompassed monitoring and evaluation of employees. By removing human discretion from organizational control systems, employees are consequently limited in their capacity to explain and contextualize the reasons for their mistakes and drops in their performance. Employees faced with the inability to appeal to the understanding of human managers may have greater concerns that they will be granted fewer exceptions for poor performance or occasional mistakes, even when they have a legitimate or justified reason. This, in turn, may also lead employees to feel greater concern that they will face increased negative consequences when AI surveillance technologies monitor them as opposed to human managers, since they are not able to explain or contextualize reasons for their mistakes or drops in their performance (Aneesh, 2009; Kellogg et al., 2020; Lee, Kusbit, Metsky, & Dabbish, 2015).

Hence, it is not only that employees are more likely to perceive monitoring by AI surveillance technologies as a greater inhibitor of their ability to control their information and interactions with others in the environment as opposed to human managers, but that employees are also more likely to think that they will face greater risks in the form of facing inflated negative consequences when AI surveillance

technologies monitor them rather than human managers due to the ubiquity of the monitoring and the inability of this form of monitoring to grant exceptions for justifiable mistakes or drops in performance. Therefore, in line with the privacy calculus model, since employees are likely to perceive monitoring by AI surveillance technologies as presenting greater risks in terms of facing negative consequences compared to monitoring by human managers, we hypothesize the following:

> *Hypothesis 1: Employees will perceive a greater invasion of their privacy when monitoring is conducted by AI surveillance technologies as opposed to human managers.*

Mediating Processes of Perceived Privacy Invasion

As stated above, the perceived risks of monitoring by AI surveillance technologies—in the form of perceived negative consequences—is likely higher than the perceived risks of monitoring by human managers because AI surveillance technologies can engage in ubiquitous monitoring and cannot grant exceptions for justifiable mistakes or drops in performance as they remove human discretion.

That is, employees' perceptions of facing greater risks in the form of perceived negative consequences when AI surveillance technologies monitor them as opposed to human managers may be explained by the ubiquity of the monitoring. For example, human managers are less likely to catch and reprimand employees every time they perform poorly or make a mistake compared to AI surveillance technology that can engage in surveillance ubiquitously, which may increase employees' concern they will face increased negative consequences when they are monitored by AI surveillance technologies. Thus, employees' perception of facing increased negative consequences

via the use of AI surveillance technologies as opposed to human managers may be explained by employees' perception of the monitoring ubiquity.

In addition to ubiquity, the replacement of human managers with AI surveillance technologies does not allow employees to appeal to the discretion of human managers who can make exceptions for justifiable mistakes or drops in performance, unlike AI surveillance technologies which cannot make exceptions. Thus, employees' perception of facing increased negative consequences via the use of AI surveillance technologies as opposed to human managers may also be explained by employees' perception that they will be granted fewer exceptions for justifiable mistakes and poor performance (Aneesh, 2009; Kellogg et al., 2020; Lee et al., 2015).

Therefore, monitoring form may shape perceived ubiquity and perceived exceptions, affecting perceived negative consequences, and may explain the relationship between monitoring form (AI surveillance technologies vs. human managers) and perceived privacy invasion as shown in figure 1.

> *Hypothesis 2: Monitoring form (AI surveillance technologies vs. human managers) effects perceived privacy invasion through perceived ubiquity, exceptions, and negative consequences. Specifically, perceived ubiquity and exceptions lead to perceived negative consequences, which subsequently leads to perceived privacy invasion.*

Insert Figure 1 about here.

The Effect of Monitoring via AI Surveillance Technologies and Privacy Invasion on Employees' Intention to Engage in Resistance Practices

The implementation and use of managerial oversight and now monitoring via AI surveillance technologies in organizations reflects a primary concern of management—the ability to control or influence the behavior of employees to ensure their behaviors fall in line with organizational goals (Flamholtz, 1996). Thus, organizational management and behavior scholars have studied the implementation and use of various organizational control systems for decades (e.g., Edwards, 1979; Gordon, Edwards, & Reich, 1982; Kellogg et al., 2020). One set of findings in this literature demonstrates that control systems can have the unintended effect of fostering counterproductive behavior or resistance practices[1] (Alge et al., 2010; Anteby & Chan, 2018; Gill, 2019; Kellogg et al., 2020; Lawrence & Robinson, 2007). Resistance practices include withholding effort (Gouldner, 1954; Roy, 1954), sabotaging company equipment (Haraszti, 1978; Juravich, 1985), avoidance or non-compliance (Anteby & Chan, 2018), strikes (McLoughlin, Badham, & Palmer, 2005), and direct criticism or complaints (Bolton, 2004; Gill, 2019), among many others. As such, AI surveillance technologies—which constitute a new form of organizational control (Kellogg et al., 2020)— may have the unintended effect of promoting counterproductive workplace behavior or resistance practices, perhaps even to a greater extent than other forms of organizational control because of their ability to

[1] Also, see supplementary materials for a description of Laurence's and Robinson's (2007) typology of resistance practices and enactments of organizational control.

inhibit employees' control and monitor ubiquitously (Alge et al., 2010; Anteby & Chan, 2018; Kellogg et al., 2020; Lawrence & Robinson, 2007).

As organizations gather information through the use of organizational control systems, such as through the use of AI surveillance technologies, employees' control over information, and therefore privacy, decreases. When employees experience a loss of privacy or control, they can become motivated to restore control, a cognitive, affective, and behavioral phenomenon known as psychological reactance (Bennett, 1998; Brehm, 1966; Brehm & Brehm, 1981). In many cases, scholars have theorized and demonstrated that employees will engage in reactance behavior that is counterproductive to the organization to reassert control (Alge et al., 2010; Anteby & Chan, 2018; Lawrence & Robinson, 2007; Yost, Behrend, Howardson, Badger Darrow, & Jensen, 2019). Importantly, as employees' perception or experience of a threat to their privacy or control increases, their motivation to restore their privacy or control (i.e., psychological reactance) also increases, making the likelihood that they will engage in behaviors in an attempt to restore their privacy or control extremely high (Brehm & Brehm, 1981; Lawrence & Robinson, 2007). Thus, the use of AI surveillance technologies may cause employees to engage in resistance practices, because the use of these ubiquitous technologies is likely to be perceived as a greater inhibitor of employees' autonomy, control, and privacy compared to oversight by human managers. Therefore, we hypothesize the following:

> *Hypothesis 3: Employees will report a greater intention to and will engage in more resistance practices when monitoring is conducted by AI surveillance technologies as opposed to human managers.*

Furthermore, the hypothesized effect of monitoring via AI surveillance technologies (as opposed to human managers) on employees' engagement in resistance practices may be due to employees' perception that their privacy is invaded to a greater extent when AI surveillance technologies monitor them as opposed to human managers. Since perceived privacy invasion is, by definition, an individual's perception that they have lost the capacity to control their information at a great cost to them (Bhave et al., 2020; Francis & Francis, 2017; Nissenbaum, 2004; Solove, 2002; Stone & Stone, 1990), and resistance practices occur when individuals attempt to restore the control that they have lost (Alge et al., 2010; Bennett, 1998; Brehm & Brehm, 1981; Lawrence & Robinson, 2007), employees' greater intention to engage in resistance practices when they are monitored by AI surveillance technologies as opposed to human managers may be due to employees' perceived privacy invasion. Therefore, we hypothesize the following:

> *Hypothesis 4: Perceived privacy invasion will mediate the relationship between the form of monitoring (AI surveillance technologies vs. human managers) and employees' intention to and engagement in resistance practices.*

Overview of Studies

We test our hypotheses across four studies. In Study 1, we examined whether participants who imagined being monitored by AI surveillance technologies were more likely to perceive an invasion of their privacy (H1) and report an intention to engage in resistance practices than participants who imagined being monitored by human managers (H3). We further examined if perceived privacy invasion explains

the relationship between monitoring form (AI surveillance technologies vs. human managers) and intention to engage in resistance practices (H4).

In Study 2, we replicated the results of Study 1 in a behavioral study. Specifically, we investigated if participants who were monitored by AI surveillance technologies were more likely to perceive an invasion of their privacy (H1) and engage in resistance practices (H3) than participants who were monitored by a research assistant. We further examined if perceived privacy invasion explains the relationship between monitoring form (AI surveillance technologies vs. human managers) and intention to engage in resistance practices (H4).

In Study 3, we again replicated the main effect of perceived privacy invasion (H1) and investigated our hypothesized mechanisms (H2). Specifically, we investigated whether participants who imagined being monitored by AI surveillance technologies were more likely to perceive an invasion of their privacy, greater monitoring ubiquity, decreased exceptions, and inflated negative consequences than participants who imagined being monitored by human managers. We then assessed whether perceived ubiquity, exceptions, and negative consequences explain the relationship between monitoring form (AI surveillance technologies vs. human managers) and perception of privacy invasion.

In Study 4, we examined ways to attenuate the main effect perceived privacy invasion by the use of monitoring by AI surveillance technologies. Specifically, we examined if framing AI surveillance technologies as developmental would reduce participants' perceived privacy invasion when AI surveillance technologies monitor them as opposed to human managers, as it may decrease participants' concern of

facing inflated negative consequences and subsequently add a benefit to the privacy calculus (Bhave et al., 2020; Culnan & Armstrong, 1999; Laufer & Wolfe, 1977). Throughout these studies, we extend prior theory to provide insight into the implications of the increasing use of AI surveillance technologies in organizations—answering calls from management scholars to empirically investigate the differences between AI surveillance technologies and human managers (Bernstein, 2017; Bhave et al., 2020; Kellogg et al., 2020).

Insert Figure 2 about here.

Study 1

To test Hypotheses 1, 3, and 4, in this study, we asked participants to imagine working in an organization in which they were monitored by either AI surveillance technologies or by human managers. We then measured participants' perception of privacy invasion, intention to engage in resistance practices, and their perceptions of the purpose of the monitoring. We predicted that participants who were monitored by AI surveillance technologies would perceive their privacy was invaded to a greater extent and would report a greater intention to engage in resistance practices. We also added an exploratory measure in which asked participants to tell us what purpose they thought the monitoring served since it is commonly examined in the literature, and we were curious whether participants would perceive the purpose of the monitoring by AI surveillance technologies differently than the purpose of monitoring by human managers.

Methods

Participants. We recruited 157 participants (56.7% female, 42.6% male; M_{age} = 19.14, SD_{age} = 1.53; 51% Caucasian) from a large research university in the Northeastern United States. For taking part in the experiment, the participants received partial course credit.

Procedure. Participants arrived at the laboratory where they were seated at a computer to begin the study. At the beginning of the experiment, participants were shown instructions informing them they would be asked to read a scenario and then answer a few multiple-choice questions about it. After the directions, participants were randomly presented with either the AI surveillance technologies monitoring scenario or the human manager monitoring scenario.

The Scenario and Monitoring Source Manipulation. All participants read the following scenario:

> You work at a casino in Las Vegas as a waitstaff member serving food and drinks. The hotel senior management team wants to ensure you are smiling and positive when you interact with guests.

Then participants randomly assigned to the AI surveillance technologies monitoring condition were notified:

> Thus, *you are monitored by video and facial recognition technologies that track and analyze your facial expressions* to ensure you are smiling and positive when you interact with guests.

Conversely, participants randomly assigned to the human manager monitoring condition were notified:

> Thus, *you are monitored by an onsite manager who observes your interactions* with guests to ensure you are smiling and positive.

Participants were then asked to fill out the primary measures, which included an attention check in which they had to report how the company ensures waitstaff members are smiling and positive when they interact with guests (1= video and facial recognition technology, 2= onsite manager, 3= secret shopper, or 4=not applicable).

Perceived Privacy Invasion. To measure participants' perceived privacy invasion, we used a pre-established 11-item scale (Alge, 2001). Example items include: "I feel like the manner in which I am evaluated is an invasion of my privacy" and "I feel that the methods used to monitor my performance are invasive." These items were rated on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*). The Cronbach's alpha for this scale was .90.

Intention to Engage in Resistance Practices. We measured participants' intention to engage in resistance practices with four items that capture resistance by non-compliance from a pre-established scale (Spitzmüller & Stanton, 2006). We slightly adapted the items to fit the scenario. Example items include: "I would try to avoid the areas of the casino that are monitored by the [video and facial recognition monitoring system/onsite manager]" and "I would encourage my co-workers to critically discuss the [video and facial recognition monitoring system/onsite manager] with their supervisor and/or the department responsible." These items were rated on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*). The Cronbach's alpha for this scale was .77.

Perceived Monitoring Purpose. Additionally, we measured participants' perception of the purpose of the company's monitoring practices as an exploratory measure since it is commonly examined in the literature, and we were curious whether

participants would perceive the purpose of the monitoring by AI surveillance technologies differently than the purpose of monitoring by human managers. We thought that AI technologies might be seen as less developmental because employees may be concerned about facing increased negative consequences by the use of this form of monitoring; therefore, employees may be more likely to see the purpose of the monitoring as punitive rather than developmental.

We used a pre-established 6-item scale (Wells, Moorman, & Werner, 2007). The 6-item scale was split into two subscales, with three items measuring participants' perception of a developmental monitoring purpose intended to aid their improvement, and three items measuring participants' perception of a deterrent monitoring purpose intended to prevent undesirable behavior. We again slightly adapted the items to fit the scenario. Example items include: "The company uses the [video and facial recognition monitoring system/onsite manager] to help employees' perform their job(s) better" and "The company uses the [video and facial recognition monitoring system/onsite manager] to prevent wrongdoing by [company] employees. These items were rated on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*). The Cronbach's alpha for the developmental monitoring purpose scale was .67, and .84 for the deterrent monitoring purpose scale.

Results

Perceived Privacy Invasion. Consistent with Hypothesis 1, participants who were monitored by the AI surveillance technologies perceived their privacy was significantly more invaded (M = 5.21, SD = 1.02) than participants who were

monitored by human managers (M = 4.66, SD = 1.10), b = 0.28, t(155) = 3.30 , p = .001 , d = 0.52.

Intention to Engage in Resistance Practices. Consistent with Hypothesis 3, participants who were monitored by the AI surveillance technologies reported a significantly greater intention to engage in resistance practices (M = 4.59, SD = 1.33) than participants who were monitored by human managers (M = 4.13, SD = 1.25), t(155) = 2.27, b = 0.84, p = .025, d = 0.36. We then tested to see whether perceived privacy invasion mediated the relationship between monitoring form (AI surveillance technologies vs. human managers) and intention to engage in resistance practices. When monitoring form and perception of privacy invasion were entered into a multiple regression model, perceived privacy invasion was significant, b = .84, p < .001, and the direct effect of monitoring form was no longer significant b = .00, p = .998. We ran a bootstrapping analysis using PROCESS Model 4 (Hayes, 2018) with 10,000 iterations to calculate the confidence interval for the indirect effect through perceived privacy invasion. The indirect effect through perceived privacy invasion was significant, 95% CI [0.09, 0.39], so there was mediation, supporting Hypothesis 4. Thus, it seems as though the increased intention to engage in resistance practices may be explained by higher perceptions of privacy invasion. The mediation diagram can be found in Figure 3.

Insert Figure 3 about here.

Perceived Monitoring Purpose. Participants who were monitored by the AI surveillance technologies perceived the company was significantly less likely to use the monitoring for developmental purposes (M = 4.34, SD = 1.20), than participants who were monitored by human managers (M = 4.78, SD = 1.14), $t(155) = -2.36$, p = .020, d = 0.38. However, participants who were monitored by the AI surveillance technologies did not perceive that the company was significantly more likely to use the monitoring for deterrent purposes (M = 5.34, SD = 1.10) than participants who were monitored by human managers (M = 5.54, SD = 1.18), $t(155) = -1.14$, p = .26, d = 0.18 . There are two potential reasons for this result. First, participants may think that management will use any form of monitoring for deterrent purposes in order to prevent unwanted behavior. Second, the pre-established scale used to capture perceptions of a deterrent monitoring purpose may not have fit the context of our scenario.

Discussion

The results of this study reveal that, consistent with Hypothesis 1, hypothetical employees felt a greater invasion of privacy when they were monitored by AI surveillance technology. Additionally, consistent with Hypothesis 3, hypothetical employees reported a greater intention to engage in resistance practices when they were monitored by AI surveillance technology. We also found evidence that hypothetical employees' greater intention to engage in resistance practices was explained by their greater sense of privacy invasion, consistent with Hypothesis 4. Moreover, hypothetical employees perceived that the company was less likely to use

monitoring by AI surveillance technology for developmental purposes, but not deterrent purposes, than monitoring by a human manager.

Study 2

The goal of Study 2 was to replicate and advance the results of Study 1 by examining downstream consequences on behavior rather than just intentions. In this study, participants were asked to participate in a creativity task while they were monitored by either AI surveillance technologies or by a research assistant. We then measured participants' perception of privacy invasion, engagement in resistance practices to test our hypotheses, and we also measured performance on the creativity task, stress, and job satisfaction, as these are other constructs that have been studied in the monitoring literature (e.g., Alge & Hansen, 2014). We predicted that participants who were monitored by AI surveillance technologies would perceive a greater invasion of their privacy (H1) and engage in more resistance practices (H3) than participants who were monitored by a research assistant. We further predicted that perceived privacy invasion would mediate the relationship between the source of monitoring (AI surveillance technologies vs. a research assistant) and engagement in resistance practices (H4).

Methods

Participants. We recruited 104 participants (61.6% female, 37.5% male, M_{age} = 19.16, SD_{age} = 1.64, 47.1% Caucasian, 85.6 % prior work experience) from a large research university in the Northeastern United States. For taking part in the experiment, the participants received partial course credit.

Procedure and Monitoring Source Manipulation. Participants completed the experiment in groups constructed on Zoom—a conference software system. The groups were randomly assigned to either the AI surveillance technologies monitoring condition or the human monitoring condition and were asked to complete a creativity task in which they had to come up with slogans to recruit applicants to their university. At the beginning of the experiment the participants arrived in the main conference video room. The participants who were assigned to the AI surveillance technology monitoring condition were told the following:

> Recently, Cornell University has been trying to create a new advertisement to recruit applicants. So, in this study we will ask you to come up with as many slogans as you can for Cornell University. You may not repeat slogans and you must use proper grammar. To ensure you work as productively as possible and work well as a team, AI technology will monitor your progress by utilizing the live video and audio feed. Specifically, textual analysis software will monitor your team's written output to ensure you are coming up with enough slogans that are distinct and use proper grammar. Audio analysis software will use the audio feed to analyze your conversations with team members to ensure you are working cooperatively and remain on task. Finally, video and facial analysis software will use the video feed to analyze your facial expressions to ensure you are focusing on the task and working well as a team. If the monitoring systems notice you are not coming up with enough slogans, working well as a team, or focusing on the task, a warning message will automatically be generated through the chat messaging system.

Then the participants were sent to a separate breakout room and sent a link to a group document so that they could complete the creativity task. To increase the realism of the manipulation, a fake zoom account was created that displayed “AI Technology Feed” and was able to capture their live audio and video feed. The research assistant was also able to view the group document in real time. While the participants were completing the task, a message was displayed twice (once after 3 minutes and again after 4 minutes). The message was broadcasted into their video conferencing room and

stated “Automatic Message: The software has indicated: You have not come up with enough creative slogans. Please try to come up with more creative slogans.” After ten minutes, the research assistant entered the breakout room and sent a Qualtrics link so the participants could fill out the measures.

The participants who were assigned to the human monitoring condition were told the following:

> Recently, Cornell University has been trying to create a new advertisement to recruit applicants. So, in this study you will be asked to come up with as many slogans as you can for Cornell University. You may not repeat slogans and you must use proper grammar. To ensure you work as productively as possible and work well as a team, I will monitor your progress by coming into the breakout room and chatting with you. Specifically, I will observe your team's written output to ensure you are coming up with enough slogans that are distinct and use proper grammar. I will also check in to ensure you are working cooperatively as a team and remain on task. Finally, I will check on your demeanor to ensure you are focusing on the task and working well as a team. If I notice you are not coming up with enough slogans, working well as a team, or focusing on the task, I will give you a warning.

Then the participants were sent to a separate breakout room and given a link to a group document so that they could complete the creativity task. While the participants were completing the task, the research assistant entered the breakout room twice (once after 3 minutes and again after 4 minutes) and told the participants, “I am here to monitor your progress.” Then the research assistant viewed their group document which contained their responses and stated, “You have not come up with enough creative slogans. Please try to come up with more creative slogans.” After ten minutes, the research assistant entered the breakout room a final time and sent a Qualtrics link so the participants could fill out the measures.

Perceived Privacy Invasion. To measure participants' perceived privacy invasion, we again used the same pre-established 11-item scale (Alge, 2001) as we used in Study 1. Example items include: "I feel like the manner in which I am evaluated is an invasion of my privacy" and "I feel that the methods used to monitor my performance are invasive." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree).* The Cronbach's alpha for this scale was .93.

Resistance Practices. To capture participants' engagement in resistance practices, we provided participants an opportunity to give feedback about the study. We then coded their responses for "open-critique" or direct criticism of the monitoring, a resistance practice that is commonly documented in the literature (Bolton, 2004; Gill, 2019).

Performance. To assess participants' performance on the creativity task, we measured the number of responses the participants generated at the group level.

Stress. To measure participants' stress, we adapted 5-items from a pre-established scale (Aiello & Kolb, 1995). Example items include: "I felt stressed when working on the slogan task" and "I felt uptight when working on the slogan task." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree).* The Cronbach's alpha for this scale was .87.

Job Satisfaction. To measure participants' job satisfaction, we adapted 4-items from the "Brief Index of Affective Job Satisfaction" (Thompson & Phua, 2012). Example items include: "I found real enjoyment in the slogan task" and "I liked the slogan task more than the average person." These items were rated on a 7-point Likert

scale *(1 = strongly disagree, 7 = strongly agree).* The Cronbach's alpha for this scale was .84.

Results

Perceived Privacy Invasion. As we predicted, participants who were monitored by the AI surveillance technologies perceived their privacy was significantly more invaded (M = 3.85, SD = 1.15) than participants who were monitored by the research assistant (M = 2.89, SD = .91), $t(102) = 4.713$, $p < .001$, d =.93.

Resistance Practices. As we predicted, a chi-squared test of independence revealed that participants who were monitored by the AI surveillance technologies complained significantly more about the monitoring form (36%) than participants who were monitored by the research assistant (9.3%), $\chi_2(1,104) = 10.778$, p =.001, Cramer's V=.322. Examples of complaints include, "…this type of AI is a gross invasion of privacy…We should be able to speak and work freely" and "…I was uncomfortable with the idea that even my facial expressions could be recorded." We then tested to see whether perceived privacy invasion mediated the relationship between monitoring form (AI surveillance technologies vs. research assistant) and engagement in resistance practices. When monitoring form and perception of privacy invasion were entered into a multiple regression model, perceived privacy invasion was significant, b = .83, p =.002, and the direct effect of monitoring form was no longer significant b = .52, p = .087. We ran a bootstrapping analysis using PROCESS Model 4 (Hayes, 2018) with 10,000 iterations to calculate the confidence interval for the indirect effect through perceived privacy invasion. The indirect effect through

perceived privacy invasion was significant, 95% CI [.14, .82], so there was mediation, supporting Hypothesis 4. Thus, it seems as though the increased engagement in resistance practices may be explained by higher perceptions of privacy invasion. The mediation diagram can be found in Figure 4.

Insert Figure 4 about here.

Performance. The participant groups who were monitored by the AI surveillance technologies came up with significantly fewer responses (M = 16.15, SD = 8.35) than the participants groups who were monitored by the research assistant (M = 25.50, SD = 9.25), $t(23) = -2.656$, $p = .014$, $d = 1.12$. The results did not change when we controlled for group size.

Stress. There was no significant difference in stress between participants who were monitored by the AI surveillance technologies (M = 3.57, SD = 1.25) and participants who were monitored by the research assistant (M = 3.68, SD = 1.21), $t(102) = -.454$, $p = .651$, $d = .09$.

Job Satisfaction. Participants who were monitored by the AI surveillance technologies reported significantly lower job satisfaction (M = 3.54, SD = 1.25) than participants who were monitored by the research assistant (M = 4.03, SD = 1.08), $t(102) = -2.157$, $p = .033$, $d = .43$.[2]

[2] We reanalyzed the data with mixed models with a random intercept for group size, and it seemed that there were some group effects (the ICCs ranged from .11 to .17), but the results remained the same. Specifically, participants who were monitored by the AI technologies reported increased privacy invasion, decreased job satisfaction, and similar stress as participants who were monitored by the research assistant.

Discussion

The results of this study reveal that, consistent with Hypothesis 1, participants felt a greater invasion of privacy when they were monitored by AI surveillance technology. Additionally, consistent with Hypothesis 3, participants engaged in more resistance practices when they were monitored by AI surveillance technology. We also found evidence that participants' greater engagement in resistance practices was explained by their greater sense of privacy invasion, consistent with Hypothesis 4. Moreover, participants' performance decreased, and they reported lower job satisfaction when they were monitored by AI surveillance technologies. However, participants who were monitored by AI surveillance technologies did not report differences in stress compared to participants who were monitored by the research assistant.

Study 3

The goals of Study 3 were to replicate the invasion of privacy results of Study 1 and to test our hypothesized mechanisms—Hypothesis 2. In a separate study, we asked participants (246) an open-ended exploratory question regarding the perceived advantages and disadvantages of monitoring via AI surveillance technology, which provided initial support for our hypothesized mechanisms. Out of the 246 participants, 205 participants discussed disadvantages of monitoring via AI surveillance technology: 92 participants described concerns of being granted fewer exceptions for justifiable mistakes or drops in performance as a disadvantage, 81 participants described concerns of facing inflated negative consequences as a disadvantage, and 45

participants described the monitoring ubiquity as a disadvantage (see Figure 5 for full results).

Insert Figure 5 about here.

With initial support for our hypothesized mechanisms, we aimed to further test our hypothesized mechanisms in an experimental study. To do this, we again asked participants to imagine working in an organization in which they were monitored by either AI surveillance technologies or by human managers. We then measured participants' perceptions of privacy invasion, perceptions of monitoring ubiquity, perceptions of exceptions, and perceptions of facing negative consequences. We predicted that participants who were monitored by AI surveillance technologies would perceive that their privacy was invaded to a greater extent than participants who were monitored by human managers. We also predicted that participants who were monitored by AI surveillance technologies would perceive greater monitoring ubiquity, a lower likelihood of being granted exceptions, and a greater risk of facing negative consequences than participants who were monitored by human managers. We further predicted that perceived ubiquity, perceived exceptions, and perceived inflated negative consequences would mediate the relationship between the source of monitoring (AI surveillance technologies vs. human managers) and perception of privacy invasion. Specifically, with perceived ubiquity and exceptions leading to perceived negative consequences. This study was preregistered on AsPredicted.

Methods

Participants. We recruited 250 participants via Prolific who agreed to participate in this study in exchange for $0.60. To promote data quality and to remove bots, participants were required to be from the United States or Canada and have a minimum 95% approval rating. We also excluded participants who failed the attention check (11 participants), in which they were asked to report which condition they were in, leaving our final sample to include 239 participants (53% female, 47% male, M_{age} = 33.42, SD_{age} = 12.21, 69.9% Caucasian).

Procedure. As in Study 1, at the beginning of the experiment, the participants were shown instructions that informed them they would be asked to read a scenario and then answer a few multiple-choice questions about it. After the directions, the participants were presented with a simple attention check. Then they were randomly presented with either the AI surveillance technologies monitoring scenario or the human manager monitoring scenario.

The Scenario and Monitoring Source Manipulation. Participants were randomly assigned to one of the two conditions and were instructed to read a short scenario and answer a few multiple-choice questions. We used the same manipulation in Study 1. Participants were then asked to fill out the dependent variable measures and to report how the company ensures waitstaff members are smiling and positive when they interact with guests (1= video and facial recognition technology, 2= onsite manager, 3= secret shopper, or 4=360-degree feedback) as an attention check.

Perceived Privacy Invasion. To measure participants' perceived privacy invasion, we again used the same pre-established 11-item scale (Alge, 2001) as we

used in Studies 1 and 2. Example items include: "I feel like the manner in which I am evaluated is an invasion of my privacy" and "I feel that the methods used to monitor my performance are invasive." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree).* The Cronbach's alpha for this scale was .93.

Perceived Ubiquity. We also asked the participants about their perceptions of the monitoring source's ubiquity. To assess perceived ubiquity, we asked participants to what extent they agreed with the following items: (1) "I feel constantly observed at work by the [video and facial recognition monitoring system/onsite manager]," (2) "The [video and facial recognition monitoring system/onsite manager] will not miss any of my behaviors at work," (3) I feel watched all of the time at work by the [video and facial recognition monitoring system/onsite manager]," (4) "I feel like everything I do at work will be noticed by the [video and facial recognition monitoring system/onsite manager]." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree)*. The Cronbach's alpha for this scale was .79.

Perceived Exceptions. In addition, we assessed participants' perceptions of the likelihood they would be granted exceptions when they performed poorly or made mistakes by the company. To examine participants' perceptions of the likelihood that they would be granted exceptions, we asked participants to what extent they agreed with the following items: (1) "The company understands that everyone has a bad day," (2) "The company makes exceptions when employees have legitimate reasons for messing up," (3) "The company does not expect perfection," (4) "The company understands that no one can perform perfectly all of the time." These items were rated

on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree)*. The Cronbach's alpha for this scale was .92.

Perceived Negative Consequences. Further, we examined participants' perceptions of facing face negative consequences from the organization's monitoring practices. To assess participants' perceptions of facing negative consequences, we asked participants to what extent they agreed with the following items: (1) "The presence of the [video and facial recognition monitoring system/onsite manager] makes me worry about being negatively evaluated at work," (2) "If I have a bad day at work, it is likely I will be punished," (3) "I feel as if I will be reprimanded for every mistake I make at work," (4) "If I perform poorly at work, it is likely I will face negative consequences," (5) "I am concerned that the company's use of the [video and facial recognition monitoring system/onsite manager] will negatively affect my performance evaluation." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree)*. The Cronbach's alpha for this scale was .93.

Results

Perceived Privacy Invasion. As we predicted, participants who were monitored by the AI surveillance technologies perceived their privacy was significantly more invaded (M = 5.71, SD = .96) than participants who were monitored by human managers (M = 4.68, SD = 1.10), $t(237) = 7.696$, $p < .001$, d = 0.99.

Perceived Ubiquity. As we predicted, participants who were monitored by the AI surveillance technologies perceived that the form of surveillance was significantly more ubiquitous (M = 6.03, SD = 0.77) than participants who were monitored by human managers (M = 5.42, SD = 1.12), $t(237) = 4.87$, $p < .001$, d =0.63.

Perceived Exceptions. As we predicted, participants who were monitored by the AI surveillance technologies perceived that the company was significantly less likely to grant exceptions (M = 2.63, SD = 1.10) than participants who were monitored by human managers (M = 3.24, SD = 1.19), $t(237) = 4.13$, $p < .001$, $d = 0.54$.

Perceived Negative Consequences. As we predicted, participants who were monitored by the AI surveillance technologies perceived that their risk of facing negative consequences was significantly greater (M = 6.18, SD = 0.80) than participants who were monitored by human managers (M = 5.57, SD = 1.02), $t(237) = -5.15$, $p < .001$, $d = 0.67$.

Serial Mediation. To test our hypothesized mechanisms, we ran a serial mediation analysis to test our full model in which monitoring form (AI surveillance technologies vs. human managers) effects perceived privacy invasion through perceived ubiquity, exceptions, and negative consequences. Specifically, with perceived ubiquity and exceptions leading to perceived negative consequences as shown in Figure 6. We used PROCESS Model 80 (Hayes, 2018) with 5,000 iterations to examine the indirect effects through perceived ubiquity, perceived negative consequences, and perceived ubiquity to perceived negative consequences. The indirect effects are reported in Table 1–which provide support for Hypothesis 2, that perceived ubiquity affects participants' perceptions of privacy invasion through its effect on perceived negative consequences. Perceived ubiquity did not have a unique effect on its own, and thus ubiquity did not lead to feelings of privacy invasion outside of its effect on negative consequences. Further, perceived exceptions affect participants' perceptions of privacy invasion and also affects participants' perceptions

of perceived negative consequences, which in turn affects participants' feelings of privacy invasion. Therefore, we found support for Hypothesis 2, that participants' perceptions of monitoring ubiquity and exceptions affects participants' perceptions of facing negative consequences, which subsequently affects participants' feelings of privacy invasion.

Overall, it seems that participants may have believed that because AI surveillance technologies were able to monitor them ubiquitously, they would face inflated negative consequences (because they would be caught and reprimanded every time their performance dropped, made a mistake or were having a rough day), which then led them to perceive an invasion of their privacy. In addition, it also seems that participants may have also believed that because they were monitored by AI surveillance technologies as opposed to human managers, they would not be able to appeal to the discretion of human managers and they would then be granted fewer exceptions for performing poorly or making mistakes. As a result, they perceived that they would face inflated negative consequences, subsequently leading them to perceive an invasion of their privacy. Of course, mediation analyses are limited, and we cannot be confident in the causal order of our mediators and dependent variable. However, we believe that this order of variables has the strongest theoretical support, and our results were supportive of this idea.

Discussion

The results of this study reveal that, consistent with Hypothesis 1 and the results from Study 1, hypothetical employees felt a greater invasion of privacy when they were monitored by AI surveillance technology. We also found evidence that this

greater sense of privacy invasion was due to their belief that they would face increased negative consequences from the ubiquitous monitoring and decreased exceptions from the removal of human discretion, supporting Hypothesis 2.

Insert Figure 6 about here.

Insert Table 1 about here.

Study 4

The purpose of Study 4 was to investigate ways to reduce employees' perceived privacy invasion when they are monitored by AI surveillance technologies as opposed to human managers. Since we found that employees' perceptions of facing negative consequences mediated the relationship between monitoring form (AI surveillance technologies vs. human managers) and employees' perceptions of privacy invasion in Study 3, we thought that taking employees' focus of off facing negative consequences would attenuate employees' perceptions of privacy invasion. Thus, we explored if framing the use of AI surveillance technologies as having a developmental purpose would add a benefit to the privacy calculus and reduce employees' concern about facing negative consequences. Theoretically, framing the use of AI surveillance technology as developmental—to help employees improve and reach their highest potential—could reduce employees' perception that they would face greater negative consequences when they are monitored by AI surveillance technologies, since the use

of this form of monitoring would not be intended to catch and punish employees when they perform poorly or make mistakes. Reducing employees' perception of facing greater negative consequences would reduce their perception of privacy invasion, since employees perceive a greater sense of privacy invasion when they are monitored by AI surveillance technologies (as opposed to human managers), because they perceive monitoring by AI surveillance technologies presents greater risks in the form of facing increased negative consequences.

In light of Studies 1–3 in which we show that employees' perceptions of privacy invasion are greater when monitored by AI surveillance technologies as opposed to human managers, and in light of the fact that the use of AI surveillance technologies is ever-present in contemporary organizational settings (American Management Association, 2007), examining ways to reduce employees' perceptions of privacy invasion when monitored by AI surveillance technologies is of upmost importance.

Therefore, we again asked participants to imagine working in an organization in which they were monitored by either AI surveillance technologies, developmental AI surveillance technologies, or by human managers. We then measured participants' perceived privacy invasion and asked several exploratory questions. We predicted that participants who were monitored by AI surveillance technologies would perceive their privacy to be invaded to a greater extent than participants who were monitored by a human manager. Additionally, we predicted that participants who were monitored by AI surveillance technologies would perceive their privacy to be invaded to a greater extent than participants who were monitored by AI surveillance technologies that were

framed as having a developmental purpose. This study was preregistered on AsPredicted.

Methods

Participants. We recruited 383 participants via Prolific who agreed to participate in this study in exchange for $0.64. To promote data quality and to remove bots, participants were required to be from the United States or Canada and have a minimum 95% approval rating. We also excluded participants who failed the attention checks (132 participants), in which they were asked to report which condition they were in, leaving our final sample to include 251 participants (46.6% female, 51.4% male, M_{age} = 32.41, SD_{age} = 11.51, 64.39% Caucasian).

Procedure. As in the previous studies, at the beginning of the experiment, the participants were shown instructions that informed them that they would be asked to read a scenario and then answer a few multiple-choice questions about it. After the directions, the participants were presented with a simple attention check. Then they were randomly presented with either the human manager monitoring scenario, the AI surveillance technologies monitoring scenario, or the developmental AI surveillance technologies monitoring scenario.

The Scenario and Monitoring Source Manipulation. All participants read the following scenario:

> You work at a large healthcare consulting firm. You help health care companies identify ways to cut costs and improve efficiency to increase profits. For example, during a typical workday, you conduct analyses on company data and create reports on your findings and suggestions for improvement for business partners.

> The company wants to ensure you work as efficiently as possible while also ensuring the quality of your work.

Participants in the human manager condition were then presented with the following information:

> Thus, **you are monitored by an onsite manager** who calculates the average time it takes you to complete a variety of tasks, measures moments of your peak performance, tracks your activities to flag and reduce distractions that impact your workflow and productivity, and records when your projects appear to be going off track.

Conversely, participants in the AI surveillance technology condition were presented with the same information as the participants in the human manager condition, but were told they were monitored by AI technologies as opposed to a human manager:

> Thus, **you are monitored by AI technologies** that automatically calculate the average time it takes you to complete a variety of tasks, measure moments of your peak performance, track your activities to flag and reduce distractions that impact your workflow and productivity, and record when your projects appear to be going off track.

Finally, participants in the developmental AI surveillance technology condition were presented with the same information as the participants in the AI surveillance technology condition, but were also presented with the additional following information:

> **The main purpose of implementing the AI technologies is for developmental reasons.** Specifically, the company wants to help employees reach their highest potential by looking for, identifying, and teaching employees ways to improve their work performance.

All participants were then asked to fill out the dependent variable measures and to report how the company ensures they work as efficiently as possible while also ensuring the quality of their work (1 = AI technologies, 2 = Onsite manager, 3 =

Quarterly evaluations, or 4 = 360-degree feedback) as an attention check. Participants were also asked to report if they read the following statement earlier in the study: "**The main purpose of implementing these types of technologies is for developmental reasons**. Specifically, the company wants to help employees reach their highest potential by looking for, identifying, and teaching employees ways to improve their work performance." Participants then selected yes or no as a second attention check.

Perceived Privacy Invasion. To measure participants' perceived privacy invasion, we again used the same pre-established 11-item scale (Alge, 2001) as we used in Studies 1-3. Example items include: "I feel like the manner in which I am evaluated is an invasion of my privacy" and "I feel that the methods used to monitor my performance are invasive." These items were rated on a 7-point Likert scale *(1 = strongly disagree, 7 = strongly agree).* The Cronbach's alpha for this scale was .95.

Manipulation checks. To test whether participants perceived the monitoring by AI surveillance technologies that were framed as having a developmental purpose as less punitive (i.e., not intended to catch and punish employees every time they make a mistake or perform poorly, or to increase negative consequences) and as more developmental (i.e., intended to help employees improve and reach their highest potential) compared to monitoring by AI surveillance technologies that were not framed as having a developmental purpose and monitoring by human managers, we assessed participants' perception of the purpose of the monitoring. Specifically, participants were asked, "To what degree do you think the company uses the [AI technologies/onsite manager] for punitive reasons? (e.g., to catch and punish

employees for making mistakes or performing poorly). And, "To what degree do you think the company uses the [AI technologies/onsite manager] for developmental reasons? (e.g., to identify and teach employees ways to improve their work performance)." These items were rated on two separate 5-point Likert scales (1 = None at all, 5 = A great deal).

Results

Manipulation checks. A one-way ANOVA showed that there were differences in participants' perception of the purpose of the monitoring as punitive, $F(2,247) = 7.23$, $p = .002$. Contrasts showed that the participants who were monitored by AI technologies with a developmental justification ($M = 3.25$, $SD = 1.05$) perceived the purpose of the monitoring was significantly less punitive than participants who were monitored by AI technologies without a developmental justification ($M = 3.86$, $SD = 1.34$), $t(247) = 3.53$, $p < .001$. Further, participants who were monitored by AI technologies with a developmental justification ($M = 3.25$, $SD = 1.05$) perceived the purpose of the monitoring as marginally less punitive than participants who were monitored by human managers ($M = 3.54$, $SD = 1.12$), $t(247) = 1.81$, $p = .072$.

Additionally, a one-way ANOVA showed that there were differences in participants' perception of the purpose of the monitoring as developmental, $F(2,247) = 7.83$, $p = .001$. Contrasts showed that the participants who were monitored by AI technologies with developmental justification ($M = 3.18$, $SD = 1.06$) perceived the purpose of the monitoring as significantly more developmental than participants who were monitored by AI technologies with a developmental justification ($M = 2.74$, $SD = 0.97$), $t(247) = 3.58$, $p < .001$. Further, participants who were monitored by AI

technologies with a developmental justification (M = 3.18, SD = 1.06) perceived the purpose of the monitoring as significantly more developmental than participants who were monitored by human managers (M = 2.82, SD = 0.96), $t(247) = 3.05$, $p = .003$.

Thus, the developmental framing manipulation was successful as participants who were monitoring by AI surveillance technologies that were framed as having a developmental purpose perceived the monitoring was less punitive and more developmental than participants who were monitored by AI surveillance technologies without a developmental framing and participants who were monitored by human managers.

Perceived Privacy Invasion. As we predicted, a one-way ANOVA showed that there were differences in participants' perceived privacy invasion by condition, $F(2,248) = 3.35$, $p = .037$. Contrasts showed that the participants who were monitored by AI technologies without a developmental justification (M = 5.26, SD = 1.07) perceived their privacy to be significantly more invaded than participants who were monitored by the human managers (M = 4.75, SD= 1.25), $t(248) = 2.56$, p =.011, d = .44. Further, participants who were monitored by the AI technologies without a developmental justification (M = 5.26, SD = 1.07) perceived their privacy was marginally more invaded than participants who were monitored by AI technologies with a developmental justification (M = 4.91, SD = 1.22), $t(248) = 1.82$, $p = .070$, d=.30.

Discussion

The results of this study reveal, consistent with Hypothesis 1 and the results of Studies 1–3, hypothetical employees felt a greater invasion of privacy when they were

monitored by AI surveillance technologies as opposed to human managers. We also found that hypothetical employees perceived their privacy to be invaded to a lesser extent (albeit marginal) when they were monitored by AI surveillance technologies that were framed as developmental than AI surveillance technologies without a developmental framing. Thus, framing monitoring by AI surveillance technologies as developmental is one possible way to attenuate employees' perceived privacy invasion.

General Discussion

In this paper we explored how AI surveillance technologies—a novel and increasingly popular form of monitoring in organizations—shape employees' perceptions of privacy invasion. We extended prior theory on monitoring within organizations and perceptions of privacy invasion by exploring how the use of AI surveillance technologies impact employees' perceived privacy invasion and engagement in resistance practices. To date, research has focused on both the impact of non-technology monitoring (e.g., Edwards, 1979; Gordon et al., 1982) and the impact of non-AI technology surveillance on privacy invasion (e.g., Alge, 2001), both of which are fundamentally distinct from AI technology surveillance (Schweitzer, Ho, & Zhangd, 2018). We also answer calls from management scholars to examine the impact of AI surveillance technologies on manager-worker dynamics, with an explicit focus on extending prior theory on perceptions of privacy invasion by evaluating differences in perceived privacy invasion by AI technology versus human managers (Bernstein, 2017; Bhave et al., 2020; Kellogg et al., 2020).

In support of Hypothesis 1 we found that employees who were monitored by AI surveillance technologies (vs. human managers) perceived a significantly higher invasion of their privacy (Studies 1–4). Moreover, in support of Hypothesis 2, we found that perceived ubiquity, perceived exceptions, and perceived negative consequences explained the relationship between monitoring form (AI surveillance technologies vs. human managers) and perceived privacy invasion. In Study 3, we found evidence that monitoring by AI surveillance technologies (as opposed to human managers) led participants to perceive that the monitoring was ubiquitous and be concerned that they would face more negative consequences for poor performance. The effect of ubiquity on privacy invasion seemed to operate through perceptions of inflated negative consequences. Participants realized that AI surveillance technologies would continuously be monitoring and recording their behavior, unlike human management who does not have the ability to catch everything, making them seemed worried that they would face negative consequences. In addition, we found evidence that monitoring by AI surveillance technologies (as opposed to human managers) led participants to perceive that they would be granted fewer exceptions for justifiable poor performance or mistakes, consequently leading to concerns that they would face more negative consequences for poor performance. Participants realized that when they were monitored by AI surveillance technologies as opposed to human managers, they would not be able to appeal to the discretion and understanding of human managers to explain and contextualize the reasons for their mistakes or poor performance. Faced with the inability to appeal to the understanding of human managers, participants had significantly greater concerns that they will be granted

fewer exceptions for justifiable poor performance or occasional mistakes. This, in turn, also led participants to feel significantly greater concern that they would face increased negative consequences by the use of AI surveillance technologies as opposed to human managers (Aneesh, 2009; Kellogg et al., 2020; Lee et al., 2015). Thus, in line with the privacy calculus model (Bhave et al., 2020; Culnan & Armstrong, 1999; Laufer & Wolfe, 1977), the perceived risks of monitoring via AI surveillance technologies—in the form of perceived negative consequences—were perceived to be higher than the perceived risks of monitoring by human managers because AI surveillance technologies can engage in ubiquitous monitoring and cannot grant exceptions for justifiable mistakes or drops in performance as they remove human discretion. Hence, participants perceived that their privacy was invaded to a significantly greater extent when monitored by AI surveillance technologies than by human managers.

Further, in support of Hypothesis 3, we found that participants who were monitored by AI surveillance technologies (vs. human managers) reported a significantly higher intention to engage in resistance practices (Study 1) and engaged in significantly greater resistance practices (Study 2). In support of Hypothesis 4, we demonstrated that participants' perceived privacy invasion explained the relationship between monitoring form (AI surveillance technologies vs. human managers) and employees' intention to engage in resistance practices (Studies 1–2). Specifically, employees' greater intention to engage in resistance practices may be explained by perceptions of their privacy being invaded—and thus, their control over their information—leading them to engage in behaviors that may restore their control (Alge

et al., 2010; Bennett, 1998; Brehm, 1966; Brehm & Brehm, 1981; Lawrence & Robinson, 2007).

Given the negative downstream consequences of employees' perceived privacy invasion for organizations, such as employees' engagement in resistance practices, in Study 4 we examined ways to attenuate hypothetical employees' perceptions of privacy invasion. We found that framing AI surveillance technology monitoring as developmental attenuated employees' perceived privacy invasion (marginally), likely because the developmental framing reduced employees' perception that they would face greater negative consequences.

Limitations and Future Directions

We found consistent evidence for the effect of monitoring form (AI surveillance technologies vs. human managers) on employees' perception of privacy invasion. However, our research is subject to several limitations and leaves many directions for future research. First, the nature of our design provides high internal validity, insofar as the monitoring source and workplace scenario manipulations across our studies involved emotionally charged, privacy-invading conditions in which participants may have equally surmised that their privacy was invaded. Thus, the fact that we found a significant difference in participants' privacy invasion between conditions provides high internal validity and is perhaps even a conservative test of otherwise larger effects observable within organizations. Future research should examine the present findings in a field setting, such as a large organization. Specifically, future research could utilize qualitative, survey, or quasi-experimental methods to examine the effects of monitoring form in an organizational setting.

Second, although the monitoring source and workplace scenario manipulations were derived from real-world examples (Peck, 2013; Schweyer, 2018), future research conducted in a field setting or a large organization could further strengthen the ecological validity of the present findings. Also, future research conducted in a field setting could examine how the effects of AI surveillance technologies on employees' perceived privacy invasion may change over time as employees get used to the monitoring.

Furthermore, future research could investigate the differences between monitoring via non-AI forms of surveillance technology and monitoring via AI surveillance technologies. The ability to equip surveillance technologies with AI fundamentally changes the nature of monitoring. Other forms of surveillance technologies that lack AI still require human oversight, because they are dependent on managerial attention and decision making (Schweitzer, Ho, & Zhang, 2018). On the contrary, AI surveillance technologies can perform and automate tasks without human support. Once the AI surveillance technology is programmed (e.g., to assess grammatical structure of all emails), then it will perform this task constantly, without human input. For example, when a manager uses a CCTV camera that is not equipped with AI to monitor employees, the manager still must watch the video attentively and make decisions regarding the employees' behavior captured by the CCTV camera. Conversely, AI surveillance technologies enable the disintermediation of human management (Kellogg et al., 2020): the replacement of managerial oversight with algorithmic oversight. That is, when a manger uses a CCTV camera equipped with AI, the manager does not need to watch the video captured by the camera, as the AI is able

to perform tasks that normally require human intelligence—the AI is able to continuously watch, analyze, and make decisions regarding employees' behavior. Thus, AI surveillance technologies fundamentally change the role of monitoring, as AI surveillance technologies, unlike monitoring by surveillance technologies without AI, removes human discretion and is not limited by human attention. Thus, future research may find differences in the effects of monitoring via non-AI forms of surveillance technology and monitoring via AI surveillance technologies.

Moreover, future research could examine additional mechanisms that explain the relationship between monitoring form (AI surveillance technologies and human managers) and employees' perceptions of privacy invasion. For example, future research could examine if differences in perceived warmth of monitoring via AI surveillance technologies and monitoring by human management explains the relationship. It is possible that perceived warmth was partially captured by perceived exceptions, which may be why it had an indirect effect on its own outside of perceived negative consequences.

Additionally, future research could increase the relevance of the present findings by examining additional potential moderators of the demonstrated effects. Considering the use of AI surveillance technologies is ever-present in contemporary organizational settings (American Management Association, 2007), investigating additional ways to attenuate employees' perceptions of privacy invasion would have profound theoretical and practical significance. Since perceived ubiquity, perceived exceptions, and perceived inflated negative consequences explain the relationship between monitoring form and perceptions of privacy invasion, future research could

investigate ways to mitigate employees' perception of ubiquity, perception of being granted fewer exceptions, and risk of facing inflated negative consequences from monitoring. For example, it is possible that limiting the ubiquity of AI surveillance technologies by affording employees more control over when and how the monitoring takes place may attenuate employees' perceptions of ubiquity. Likewise, allowing employees a chance to provide explanations for drops in performance or mistakes may also attenuate their perceptions of privacy invasion, as it may reduce their perceptions of being granted fewer exceptions and facing inflated negative consequences.

Relatedly, future research could investigate individual differences, such as privacy preferences or values (Westin, 2003), to understand further how employees make privacy-related decisions. Similarly, future research could investigate how individual differences in need for privacy (Oldham, 1988) moderate the effect of monitoring form on perceived privacy invasion.

Lastly, future research should consider how different forms of AI surveillance technology shape perceptions of privacy invasion. Some organizations have begun implementing wearable forms of AI surveillance technology (e.g., wearable tracking devices with GPS, biosensors, and accelerometers). As such, it is important to understand how invasive versus non-invasive AI technology surveillance may increase or decrease perceptions of privacy invasion.

Conclusion

Understandably, it is important for management to understand how to control or influence the behavior of employees to ensure their behaviors fall in line with organizational goals (Flamholtz, 1996). However, like other forms of organizational

control systems, the use of AI surveillance technologies can have the unintended effect of fostering counterproductive behavior—the very behavior they are attempting to control or prevent.

Furthermore, given that previous researchers have demonstrated that perceptions of privacy invasion can lead to an array of undesirable organizational outcomes, such as decreased trust (Miller & Weckert, 2000), reduced inter-organizational communication (Botan, 1996; Holton & Fuller, 2008), reduced productivity and compliance with rules and procedures (Zweig & Scott, 2007), understanding the effects of the widespread use of AI surveillance technologies is particularly important. The use of AI surveillance technologies is evermore increasing (American Management Association, 2007), and it is one of the most exciting developments for organizations in recent years. Although this technology yields many benefits, there are also unintended costs that could severely impact the future of an organization and the pursuit and accomplishment of their goals. Thus, it is crucial to understand how people perceive privacy invasion following the implementation of AI surveillance technologies, the negative downstream consequences of perceived privacy invasion from these technologies, and ways to mitigate the negative consequences. Our paper makes initial advances in understanding the relationship between AI surveillance technologies and employees' perceived privacy invasion, the consequences of this specific form of monitoring, and ways to mitigate the unintended negative consequences, demonstrating how this novel form of monitoring is fundamentally different from human managers envisioned by management scholars many years ago.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Aiello, J. R., & Kolb, K. J. (1995). Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress. *Journal of Applied Psychology*, *80*(3), 339–353. https://doi.org/10.1037/0021-9010.80.3.339

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, *86*(4), 797–804. http://doi.apa.org/getdoi.cfm?doi=10.1037/0021-9010.86.4.797

Alge, B. J., Anthony, E. A., Ress, J., Kannan, K., Neider, L., & Schriesheim, C. (2010). Controlling A, while hoping for B: Deviance and detterence and public versus private deviance. In S. Chester & L. L. Neider (Eds.), *The Dark Side of Management* (pp. 115–141). Charlotte, NC: Information Age Publishing.

Alge, B. J., & Hansen, S. D. (2014). Workplace Monitoring and Surveillance since "1984." In *The Psychology of Workplace Technology*. New York, NY: Routledge.

Allen, M. W., Walker, K. L., Coopman, S. J., & Hart, J. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172–200. https://doi.org/10.1177/0893318907306033

American Management Association, (AMA). (2007). *Electronic monitoring & surveillance survey*.

Aneesh, A. (2009). Global labor: Algocratic modes of organization. *Sociological Theory*, *27*(4), 347–370.

Anteby, M., & Chan, C. K. (2018). A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification. *Organization Science*, *29*(2), 247–263.

Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, *51*(1), 87–106.

Ball, K, Haggerty, K. D., & Lyon, D. (2012). *Routledge handbook of surveillance studies*. New York, NY: Routledge.

Ball, Kristie. (2010). Workplace surveillance: An overview. *Labor History*, *51*(1), 87–106.

Bennett, R. (1998). Perceived powerlessness as a cause of employee deviance. In A.

Griffin, O'Leary-Kelly, & J. Collins (Eds.), *Dysfunctional behavior in organizations: Violent and dysfunctional behavior* (pp. 221–239). Stamford, CT: JAI.

Bernstein, E. (2012). The transparency paradox: A role for privacy in organizational learning and operational control. *Administrative Science Quarterly*, *57*(2), 181–216.

Bernstein, E. (2014). The transparency trap. *Harvard Business Review*, *92*(10), 121–166.

Bernstein, E. (2017). Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals*, *11*(1), 217–266. https://doi.org/10.5465/annals.2014.0076

Bhave, D., Teo, L. H., & Dalai, R. (2020). Privacy at Work : A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, *46*(1), 127–164. https://doi.org/10.1177/0149206319878254

Bolton, S. C. (2004). A simple matter of control? NHS hospital nurses and new management. *Journal of Management Studies*, *41*(2), 317–333.

Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communication Monographs*, *63*(1), 233–313.

Brehm. (1966). *A theory of psychological reactance.* New York, NY: Academic Press.

Brehm, S., & Brehm, J. (1981). *Psychological reactance: A theory of freedom and control*. New York, NY: Academic Press.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Dalton, M. (1959). *Men who manage: Fusions of feeling and theory in administration*. New York, NY: Wiley.

Edwards, R. C. (1979). *Contested terrain: The transformation ofthe workplace in the twentieth century*. New York, NY: Basic Books.

Flamholtz. (1996). Effective organizational control: A framework, applications, and implications. *European Management Journal*, *14*(1), 596–611.

Francis, L., & Francis, J. (2017). Privacy: What everyone needs to know. In *Privacy: What everyone needs to know*. Oxford University Press.

Gill, M. J. (2019). The significance of suffering in organizations: Understanding variation in workers' responses to multiple modes of control. *Academy of Management Review*, *44*(2), 377–404. https://doi.org/10.5465/amr.2016.0378

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Doubleday.

Gordon, D. M., Edwards, R., & Reich, M. (1982). *Segmented work, divided workers: The historical transformation of labor in the United States*. Cambridge, MA: Cambridge University Press.

Gouldner, A. W. (1954). *Patterns of industrial bureaucracy*. Glencoe, IL: Free Press.

Haraszti, M. (1978). *A worker in a worker's state*. New York, NY: Universe Books.

Hayes, A. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Holton, C., & Fuller, R. (2008). Unintended consequences of electronic monitoring of instant messaging. *IEEE Transactions on Professional Communication*, *51*(1), 381–395.

Jewell, E., & Abate, F. (2010). *New Oxford American Dictionary* (3rd ed.; A. Stevenson & C. Lindberg, eds.). New York, NY: Oxford University Press.

Juravich, T. (1985). *Chaos on the shop floor: A worker's view of quality, productivity, and management*. Philadelphia, PA: Temple University Press.

Kantor, J., & Streitfeld, D. (2015). Inside Amazon: Wrestling big ideas in a bruising workplace. *The New York Times*.

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, *14*(1), 366–410. https://doi.org/10.5465/annals.2018.0174

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(1), 22–42.

Lawrence, T. B., & Robinson, S. L. (2007). Ain't Misbehavin: Workplace deviance as organizational resistance. *Journal of Management*, *33*(3), 378–394. https://doi.org/10.1177/0149206307300816

Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with machines: The impact of algorithmic and data-driven management on human workers. *The*

Proceedings of the 33rd Annual ACM Conferenceon Human Factors in Computing Systems.

Levinson, A. A. (2009). Industrial justice: Privacy protection for the employed. *Cornell Journal of Law and Public Policy*, *18*(18), 609–688.

McLoughlin, I. P., Badham, R. J., & Palmer, G. (2005). Cultures of ambiguity: Design, emergence and ambivalence in the introduction of normative control. *Work, Employment and Society*, *19*(1), 67–89.

McNall, L. A., & Roch, S. G. (2009). A social exchange model of employee reactions to electronic performance monitoring. *Human Performance*, *22*(3), 204–224. https://doi.org/10.1080/08959280902970385

McNall, L. A., & Stanton, J. M. (2011). Private Eyes Are Watching You: Reactions to Location Sensing Technologies. *Journal of Business and Psychology*, *26*(3), 299–309. https://doi.org/10.1007/s10869-010-9189-y

Merton, R. (1957). *Social theory and social structure*. Glencoe, IL: Free Press.

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the Internet. *Journal of Business Ethics*, *28*(1), 255–265.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158.

Oldham, R. (1988). Effects of changes in workspace partitions and spatial density on employee reactions: A quasi- experiment. *Journal of Applied Psychology*, *73*(1), 253–258.

Peck, D. (2013). They're watching you at work. *Atlantic*, pp. 72–84.

Rawlinson, K. (2013). Tesco accused of using electronic armbands to monitor its staff. *The Independent*.

Roy, D. (1954). Efficiency and "the fix": Informal intergroup relations in a piecework machine shop. *American Journal of Sociology*, *60*(3), 255–266.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 1784–1810.

Schweitzer, M. E., Ho, T.-H., & Zhang, X. (2018). How Monitoring Influences Trust: A Tale of Two Faces. *Management Science*, *64*(1), 253–270. https://doi.org/10.1287/mnsc.2016.2586

Schweyer, A. (2018). Predictive analytics and artificial intelligence in people management. In *Incentive Research Foundation*.

Smith-Butler, L. (2009). Workplace privacy: We'll be watching you. *Ohio Northern University Law Review*, *35*(1), 53–81.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326

Spitzmüller, C., & Stanton, J. M. (2006). Examining employee compliance with organizational surveillance and monitoring. *Journal of Occupational and Organizational Psychology*, *79*(2), 245–272. https://doi.org/10.1348/096317905X52607

Stone, F., & Stone, L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, *8*(3), 349–411.

Sullivan, F. &. (2017). *Wearable technologies for industrial applications: Smart glasses, wrist-worn devices, HUDs improve productivity and efficiency in industrial sector*.

Taylor, F. (1911). *The principles of scientific management*. New York, NY: Harper and Brothers.

Thompson, E. R., & Phua, F. T. T. (2012). A Brief Index of Affective Job Satisfaction. *Group and Organization Management*, *37*(3), 275–307. https://doi.org/10.1177/1059601111434201

Wells, D. L., Moorman, R. H., & Werner, J. M. (2007). The impact of the perceived purpose of electronic performance monitoring on an array of attitudinal variables. *Human Resource Development Quarterly*, *18*(1), 121–138. http://doi.wiley.com/10.1002/hrdq.1194

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(1), 431–453.

Yost, A. B., Behrend, T. S., Howardson, G., Badger Darrow, J., & Jensen, J. M. (2019). Reactance to electronic surveillance: A test of antecedents and outcomes. *Journal of Business and Psychology*, *34*(1), 71–86. https://doi.org/10.1007/s10869-018-9532-2

Zweig, D., & Scott, K. (2007). When unfairness matters most: supervisory violations of electronic monitoring practices. *Human Resource Management Journal*, *17*(3),

227–247.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior*, *23*(5), 605–633. https://doi.org/10.1002/job.157

Figure 1. Conceptual diagram of mechanisms of perceived privacy invasion.

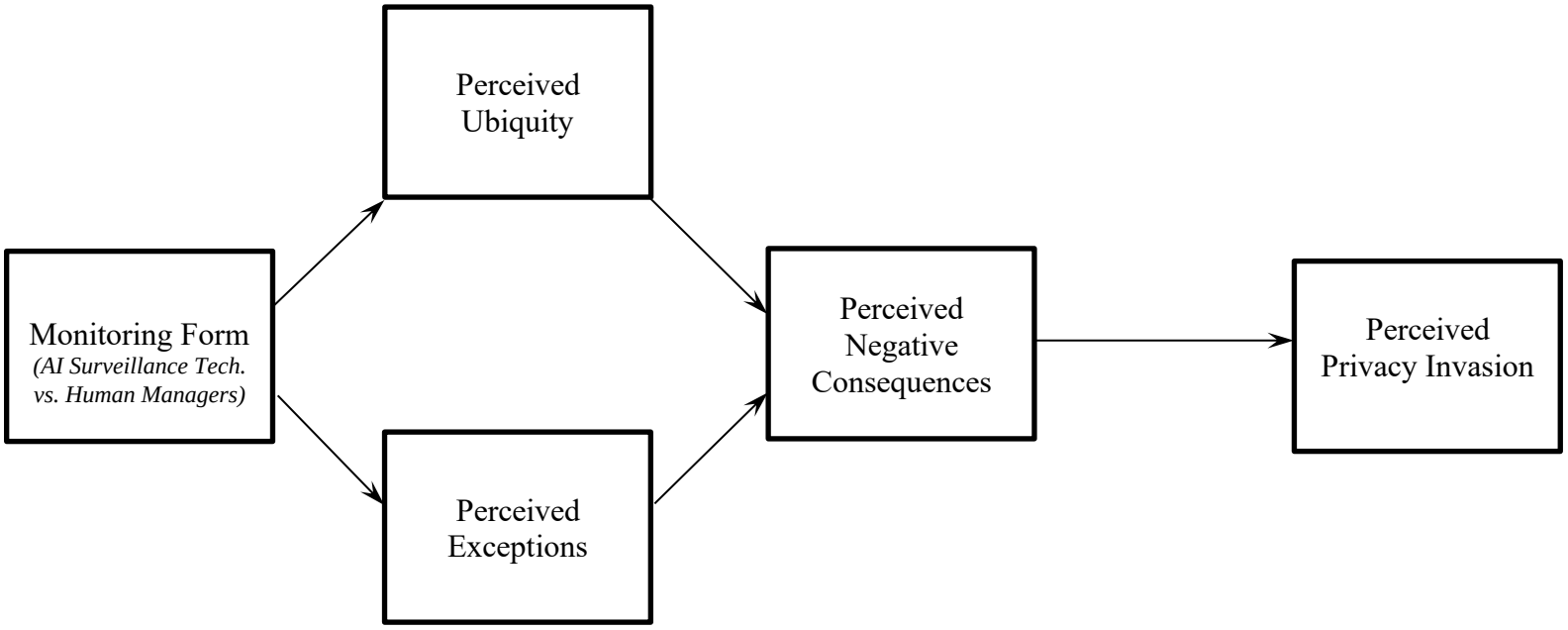

Figure 2. Conceptual diagram.

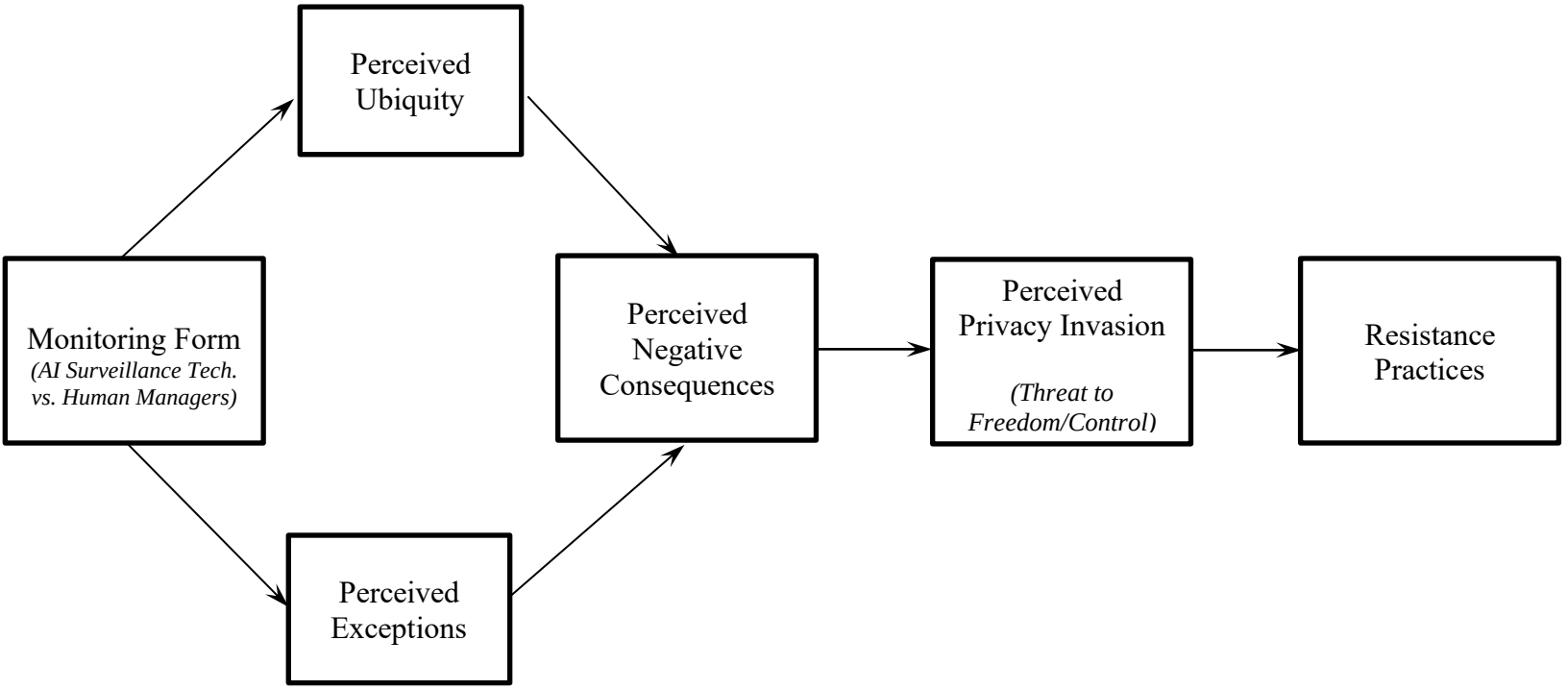

Figure 3. Mediation diagram for Study 1.

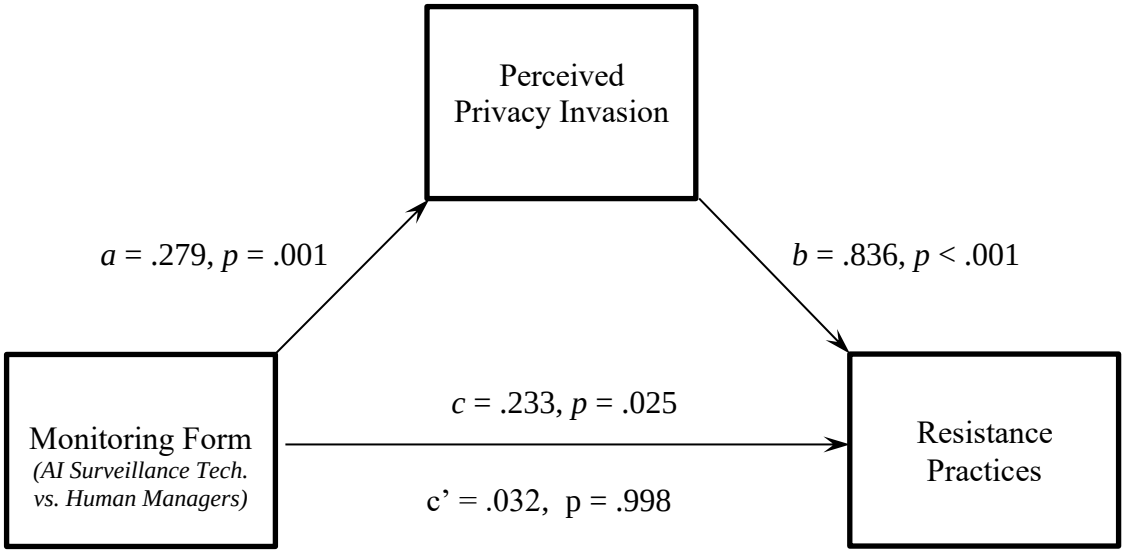

Figure 4. Mediation diagram for Study 2.

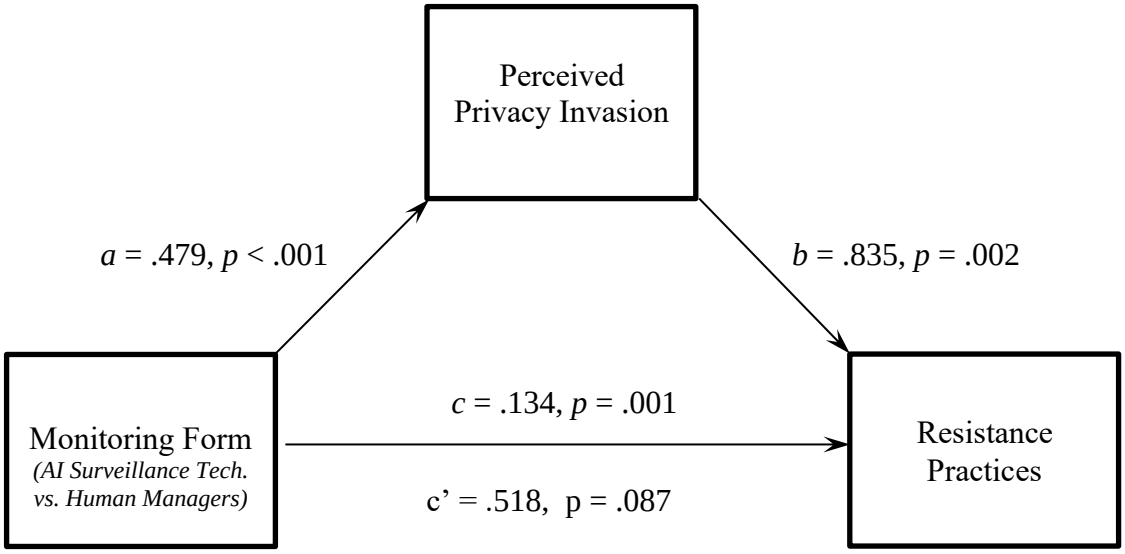

Figure 5. Frequencies of top 5 disadvantages listed of AI surveillance technology monitoring

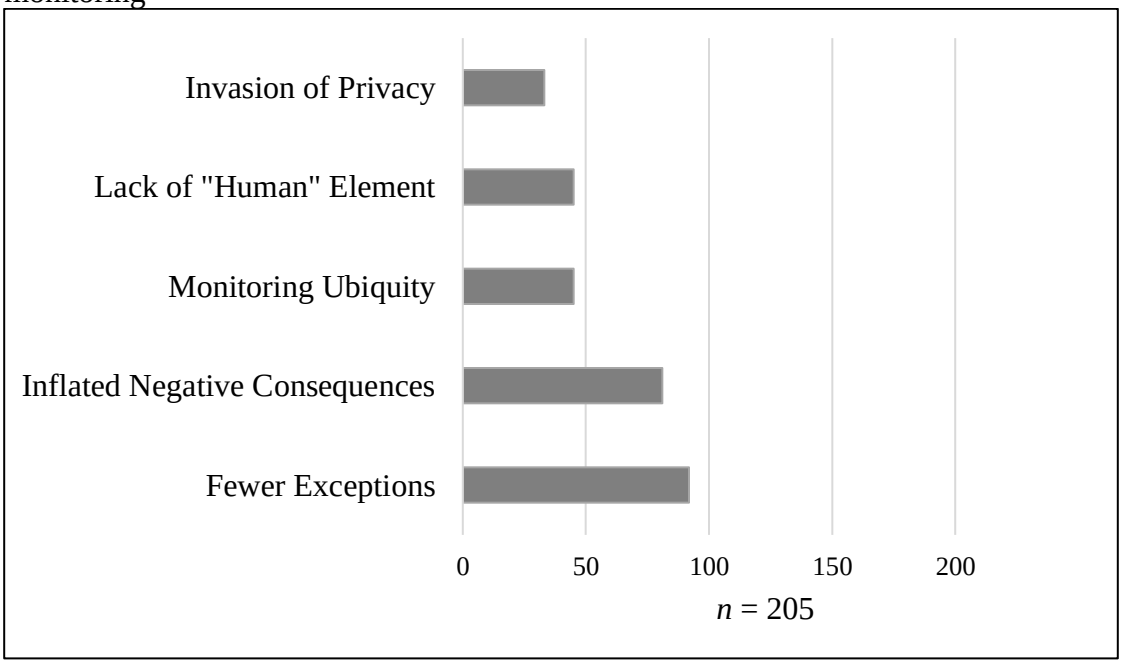

Figure 6. Mediation diagram for Study 3.

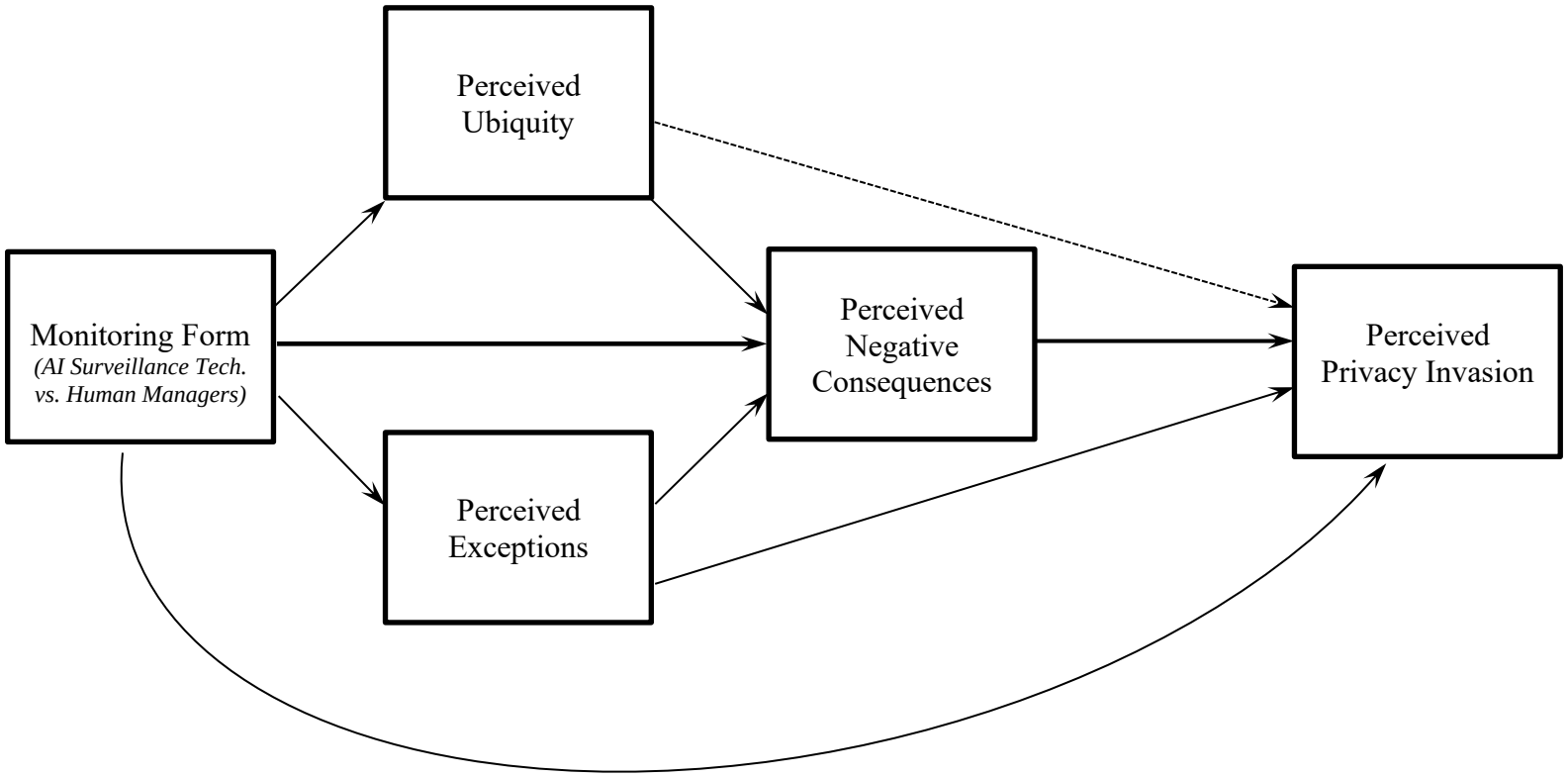

Table 1. Mediation analyses in Study 3.

				Bias Corrected 95% CI	
		Estimated Indirect Effect	***SE***	**Lower**	**Upper**
Indirect Effect 1	Ubiquity Only	.0257	.0227	-.0139	.0753
Indirect Effect 2	Exceptions Only	.0559	.0241	.0151	.1099
Indirect Effect 3	Negative Consequences Only	.0481	.0236	.0004	.0946
Indirect Effect 4	Ubiquity to Negative Consequences	.0517	.0184	.0213	.0929
Indirect Effect 5	Exceptions to Negative Consequences	.0665	.0200	.0310	.1091

N = 239; 5,000 Bootstrap Resamples

Supplementary Materials

Resistance practices occur when management enacts power over employees that provokes frustration in employees (Lawrence & Robinson, 2007). Enactments of power can provoke frustration in employees in a variety of ways, including when employees' perceive an enactment of power as a threat to their freedom and control. When employees' perceive a threat to their sense of freedom and control, and therefore, privacy, employees may become motivated to restore their freedom and control and engage in behaviors (i.e., resistance practices) in an attempt to do so (Brehm, 1966; Brehm & Brehm, 1981; Lawrence & Robinson, 2007). To describe the conditions that influence the form of resistance employees will most likely engage in, Laurence and Robinson (2007) typologies enactments of power and forms of resistance.

According to Laurence and Robinson (2007), two dimensions of power influence the form of resistance that employees will engage in. The first dimension involves what is termed "The objectification of power," while the second dimension involves what is termed "The mode of power." In addition, Laurence and Robinson (2007) propose two dimensions of resistance that include the "severity" and the "target" of the resistance. In the following section, I first define the dimensions and typology of enactments of power following Laurence and Robinson (2007). Then, I describe the two dimensions and typology of resistance also following Laurence and Robinson (2007). Finally, I will map the two concepts, explaining the conditions that influence the form of resistance employees will most likely engage in and apply the

model to the use of AI surveillance technologies and direct supervision by human managers.

The Dimensions and Typology of Power

Laurence and Robinson (2007) describe two dimensions of power that they use to topologize forms of power. The first dimension of power is termed the "Objectification of power" which involves how the enactment of power engages with the target of the power. According to Laurence and Robinson (2007), enactments of power either treat the target as a "subject" or as an "object" (Laurence & Robinson, 2007). When an enactment of power treats the target as a "subject," the target is treated as an agentic being capable of choice. For example, when an enactment of power involves the attempt to influence the target through negotiation or rational persuasion, the target of the enactment of power is treated as agentic. Direct supervision by human managers is an example of an enactment of power that treats the target as a "subject" (Laurence & Robinson, 2007). Conversely, when an enactment of power does not assume agency on behalf of the target, the enactment of power treats the target as an "object." For example, the use of AI surveillance technologies, or what Laurence and Robinson (2007) term "material technologies" does not include an attempt to influence the target and does not treat the target as agentic.

The second dimension of power is termed "the mode of power" and involves the way in which the enactment of power takes place. Enactments of power can take place in either an "episodic" or "systematic" manner (Laurence & Robinson, 2007). Enactments of power that are relatively discrete and strategic attempts can be

classified as episodic enactments of power. Conversely, enactments of power that are sustained and routine can be classified as systematic enactments of power.

Thus, when the two dimensions of power are combined, four typologies of power emerge: 1) episodic and non-objectifying forms of power, 2) episodic and objectifying forms of power, 3) systematic and non-objectifying forms of power, and 4) systematic and objectifying forms of power. Forms of power that are episodic and non-objectifying are termed "influence" and can involve enactments of power such as negotiation or ingratiation. Episodic and objectifying forms of power are termed "force" and can involve restraining or directing targets in ways that do not give the target a choice (i.e., firing or relocating an employee). Forms of power that are systematic and non-objectifying enactments of power are termed "discipline" and can involve socialization or direct observation. Finally, systematic and objectifying forms of power are termed "domination" and can involve the use of AI surveillance technologies or "material technologies" or "pay systems that discriminate."

The Dimensions and Typology of Resistance

Additionally, Laurence and Robinson (2007) describe two dimensions of resistance that they use to topologize forms of resistance. The first dimension of resistance is the "severity" of the resistance and refers to the extent to which a resistance practice violates organizational norms and is harmful to the organization or the organizations members. The severity of resistance can be classified as minor such as withholding effort or failing to show up to work, or serious such as physical violence or theft. The second dimension of resistance is the "target" of the resistance

and refers to whether the target of the resistance is the organization (i.e., organizationally directed) or its members (i.e., individually directed).

Therefore, the two dimensions of resistance topologize resistance practices into four forms of resistance: 1) minor and organizationally-directed, 2) severe and organizationally-directed, 3) minor and individually-directed, 4) severe and individually-directed. Forms of resistance that are minor and organizationally-directed are termed "production deviance "and can include behaviors such as taking excessive breaks, withholding effort, and violating norms of quality and quantity of work performance. Severe and organizationally-directed forms of resistance are termed "property deviance" and can include behaviors such as theft, failure to comply, and sabotaging equipment. Forms of resistance that are minor and individually-directed are termed "political behavior" and can involve behaviors such as gossiping or scapegoating. Finally, severe and individually-directed forms of resistance are termed "personal aggression" and can involve behaviors such as harassment and physical harm.

The Model of Power and Resistance

According to Laurence and Robinson (2007), forms of power that objectify the target increases the severity of resistance as opposed to forms of power that treat the target as a subject. Further, forms of power that are episodic tend to lead to individually-directed forms of resistance as the discrete nature of the form of power allows an individual to be identified. Moreover, forms of power that are systematic tend to lead to organizationally-directed forms of resistance as the ongoing and routine nature of the form of power does not allow an individual to be identified as easily.

Thus, applying the typologies of power and resistance, episodic and non-objectifying forms of power or "influence" tend to lead to forms of resistance that are minor and individually-directed or "political behavior." Episodic and objectifying forms of power or "force" tend to lead to severe and individually-directed forms of resistance or "personal aggression." Forms of power that are systematic and non-objectifying enactments of power or "discipline" tend to lead to forms of resistance that are minor and organizationally-directed or "production deviance." Finally, systematic and objectifying forms of power or "domination" tend to lead to severe and organizationally-directed forms of resistance or "property deviance."

Applying Laurence's and Robinson's (2007) model of enactments of power and forms of resistance, AI surveillance technologies are classified as systematic and objectifying enactments of power (i.e., domination) as they are ongoing, routine attempts to enact power over employees that treat the employees as "objects" rather than as "subjects." Thus, the use of AI surveillance technologies should lead to forms of resistances that are severe and organizationally-directed (i.e., property deviance), which can included behaviors such as theft, failure to comply, and sabotaging equipment.

Conversely, direct supervision by human management is classified as a systematic and non-objectifying enactment of power (i.e., discipline), as direct supervision by human management is ongoing and routine but treats the targets or employees as "subjects" rather than as "objects." Thus, the use of direct supervision by human management should lead to forms of resistance that are minor and organizationally-directed (i.e., production deviance) and can include behaviors such as

taking excessive breaks, withholding effort, and violating norms of quality and quantity of work performance.

Although both AI surveillance technologies and direct supervision by human managers can lead to employees' resistance, AI surveillance technologies may increase employee's engagement in resistance practices to a greater extent than monitoring by human managers. Since employees' motivation and engagement in behaviors, such as resistance practices, in an attempt to restore their privacy and control increases as their perception of a threat to their privacy and control increases (Brehm & Brehm, 1981; Lawrence & Robinson, 2007), employees may be more likely to engage in resistance practices when AI surveillance technologies monitor them as opposed to human managers. That is, since employees are likely to perceive the use of AI surveillance technologies as a greater inhibitor of their capacity to control their information; and thus privacy, than the use of monitoring by human managers, employees may also engage in more resistance practices when AI surveillance technologies monitor them as opposed to human managers.