Gadjah Mada International Journal of Business
Vol. 28, No. 2 (May 2026): 213-238

Blinking Back at Big Brother: Examining Threat Avoidance in the Face of Panoptic Surveillance

Naufal Afif[ab], *Syaiful Ali*[b]*, *Harminder Singh*[c]

[a]Accounting Department, Faculty of Economics, Universitas Tidar, Indonesia
[b]Accounting Department, Faculty of Economics and Business, Universitas Gadjah Mada, Indonesia
[c]Auckland University of Technology, New Zealand

ABSTRACT

This study applies Technology Threat Avoidance Theory (TTAT) to examine how panoptic surveillance in organizations induces avoidance intentions among professionals, with responses varying by occupational background. By employing an online 2x2 between-subjects factorial design, this study manipulated two conditions: the nature of the surveillance technology threat (panoptic vs. non-panoptic) and the efficacy of threat protection (high vs. low). This approach facilitated robust data collection on avoidance intention, the dependent variable, from 173 information technology professionals and 65 finance professionals, who were randomly allocated to distinct experimental conditions. This study found a strong primary effect (H1), showing that professionals across occupational backgrounds exhibit significantly higher avoidance intentions when faced with complex panopticon surveillance than with simpler surveillance methods. However, findings regarding the role of perceived protection effectiveness remain mixed, suggesting limitations in complex work environments. The originality of this study lies in its exploration of how technology design configurations in management control affect employees' perceptions, particularly on privacy, and its expansion of technology threat avoidance theory into the field of business. These findings provide preliminary evidence regarding the impact of surveillance on perceptions, while the mixed moderation results open up opportunities for further exploration in tailoring electronic surveillance.

Keywords: surveillance technology, panopticon, avoidance intention, TTAT
JEL Classification: M15

*Corresponding author's e-mail: s.ali@ugm.ac.id

ISSN: PRINT 1411-1128 | ONLINE 2338-7238
https://journal.ugm.ac.id/gamaijb

INTRODUCTION

Organizations can now supervise their employees more flexibly by monitoring and evaluating their performance from anywhere, at any time (Leclercq-Vandelannoitte, 2019). These technologies, often referred to by the acronym MELT (metrics, events, logs, and traces), enable organizations to easily collect and store large volumes of data for extended periods (Csapo & Brisan, 2014) and exchange information within the company instantaneously and continuously (Lemieux, 2018). Application of such advanced IT for employee supervision has proven to increase organizational efficiency, optimize managers' time (Leclercq-Vandelannoitte et al., 2014), enhance openness, and create work environments that are objective, fair, respectful, collaborative, and harmonious (Liew, 2015). Furthermore, a recent research on Indonesia's digital landscape indicates that technological advancements are expected to boost employee engagement, which, in turn, is a key driver of overall job satisfaction (Azmy, 2024). Accordingly, employees may also be more inclined to share their ideas and feedback.

However, at the same time, the increased use of technology for supervision is not an unalloyed good (Dinev et al., 2008; Hartman, 1998; Holt et al., 2017; Thiesse, 2007; Vorvoreanu & Botan, 2000). This is especially the case when new technologies, such as GPS tracking, RFID presence monitoring, and social media analysis, have the potential to shift supervision toward pervasive surveillance rather than detached oversight. The increasing availability and embeddedness of such technologies allow companies to monitor their employees by recording and continuously analyzing their activities and behavior in real time. This practice is akin to panoptic surveillance (Poster, 1990; Seele, 2016), where surveillance targets are ignorant as to whether they are being monitored, hence causing them to assume that they are constantly being watched by other parties (Brivot & Gendron, 2011) .

Amazon uses a panopticon surveillance system for its delivery staff (Royle, 2023). Cameras placed in their vehicles keep close track of various actions, such as the number of times seatbelts are buckled and unbuckled (called "seatbelt violations") and when mobile phones are connected or disconnected from Bluetooth (an indicator of driver distraction). Many Amazon drivers find this monitoring extremely intrusive and are displeased. This widespread practice of panopticon-style surveillance has given rise to the "Big Brother" metaphor, a term derived from Orwellian literature that serves as a synonym for an all-seeing authority that suppresses individual freedom through constant surveillance (Power, 2016). In this context, organizations assume the role of Big Brother, where they continuously monitor their operations through digital traces.

The implementation of panoptic surveillance, while ostensibly intended to enhance organizational efficiency and compliance, frequently engenders substantial adverse consequences, including heightened work pressure, stress, anxiety, fatigue, diminished creativity, and diminished job satisfaction (Ball, 2010; Bao et al., 2022; Dawood, 2023; Samaranayake & Gamage, 2012; Vorvoreanu & Botan, 2000). This pervasive monitoring

creates an unblinking organizational gaze akin to Big Brother, as it often conflicts with employees' well-being and autonomy. We conceptualize the resulting resistance as "blinking back," defined as the intentional disruption of this surveillance through the intent to avoid it. Just as a physical blink temporarily breaks visual contact to protect the eyes, employees "blink back" by using strategies to bypass or neutralize intrusive technologies that threaten their sense of privacy. The inherent tension between constant surveillance and employees' drive to blink back provides the impetus for this study's investigation of employees' intention to avoid technological threats.

This tension motivates this study, which explores how panoptic surveillance in an organization may prompt its employees to respond by avoiding the technologies involved and engaging in other negative behaviors. From a legal perspective, employee surveillance can occur if it is reasonable, disclosed, and proportionate (Charbonneau & Doberstein, 2020). However, these considerations are less relevant when the second-order consequences of monitoring, i.e., impaired employee well-being and a work environment lacking trust, are examined. As organizations digitize their work processes, a key aspect of their transformation is how they supervise their employees.

New technologies allow employees to work remotely or encourage firms to hire contractors to be more responsive to changes in their marketplace. However, the default managerial stance of using technology to replace face-to-face supervision may lead digital transformation initiatives to encounter employee resistance, as employees are leery of their privacy being invaded (Kensbock & Stöckmann, 2021). This resistance often occurs during the critical phases of technological innovation—particularly the diffusion phase—where user feedback and acceptance determine whether a technology can be successfully scaled within an organization (Aldianto et al., 2021). If innovation management fails to address employees' concerns, the intended digital transformation may be rejected rather than adopted. It is thus important for IS managers and decision-makers engaged in such IT projects to examine whether they are in conflict with or comply with employers' obligations to act in good faith (Galliers et al., 2017).

The theoretical framework guiding this research is the technology threat avoidance theory (TTAT) (Liang & Xue, 2009). Avoidance refers to refraining from, or escaping from, an action, person, or thing. TTAT asserts that users' avoidance intention starts with assessing the threats that arise and the precautions feasible to adopt. Once threat assessment and safeguard identification have been conducted, a motivation to avoid the information technology threat emerges, leading to avoidance intention. Using a sample of 173 IT professionals, an internet-based experiment found that avoidance intention was greater when monitoring was using the panoptic surveillance rather than with non-panoptic surveillance. A greater avoidance intention was also observed when protection effectiveness, defined as a protection system's ability to withstand an attack and deter an adversary (Vintr et al., 2012), was high, especially in panoptic surveillance contexts. In the final section of this paper, we attempt to test the instrument using a sample of respondents with non-IT occupational backgrounds (i.e., finance respondents). This is to better understand how background knowledge affects the manipulation. The results show differences between respondents with IT backgrounds and non-IT backgrounds.

This study makes two major contributions to management control literature. It recontextualizes TTAT by shifting its traditional focus from external malicious risks to threats originating from within the institution and embedded in the management control system. By exploring how panoptic surveillance triggers inherent psychological resistance,

this study reveals the phenomenon of threat-assessment dominance. Under these conditions, the fear of losing freedom and the invasion of autonomy is far stronger than logical calculations regarding how effective various forms of protection are in avoiding threats. Consequently, when selecting control instruments for digitalizing supervision, organizations should carefully balance operational efficiency with the preservation of employee privacy, rights, and trust (Christ, 2013; Fähndrich, 2023). This explains why traditional risk assessments fail when workplace monitoring becomes excessively intrusive.

Beyond theoretical considerations, this study investigates the important social and practical issues of workplace surveillance. This study contends that the choice of management control instruments should not be regarded merely as a technological option but rather a strategic alignment with global privacy rules and frameworks, such as the General Data Protection Regulation. This study provides a framework for organizations to navigate the delicate balance between operational surveillance and the erosion of organizational trust by investigating the varying influences of different professional backgrounds, particularly IT and non-IT employees, on their avoidance intentions (Mulvaney, 2019). Ultimately, this study emphasizes the need for job-specific, transparent, and ethically sound digital controls that safeguard organizational stability and promote employee psychological well-being.

This study provides evidence that employees in finance or information technology (IT) will avoid the threat posed by panopticon-based surveillance technology, one with a very complex design, and real-time surveillance technology implemented in a simple or non-panoptic manner. This study also provides empirical evidence that employees with an IT background have greater avoidance intention when protection effectiveness is high than when it is low. A deep understanding of existing safeguards means that IT employees are more evasive than finance employees. Finally, this study demonstrates that IT employees are more likely to avoid surveillance when protection effectiveness is high, rather than low, in situations involving panoptic surveillance technology.

The following section provides a literature review and hypothesis development on existing studies on the threat of panopticon surveillance. Section 3 describes the research methods applied to collect and analyze the data. Section four discusses the test results, followed by a discussion of the results. The next section is Study 2, testing with different respondents. The last section is this research's conclusion, limitations, and future studies.

BACKGROUND LITERATURE AND HYPOTHESIS DEVELOPMENT

The Threat of Surveillance Technology by Panopticons

Jeremy Bentham conceptualized the panopticon, a prison design, in the late 18th century (Bentham, 1791). Bentham's panoptic architecture consists of two structural elements. The first building on the outskirts was circular, with expansive windows leading to the center and windows for outward lighting. Meanwhile, the other building sits in the center of a circular-shaped building and has an open window to enable guards to watch the prisoners. This design allows guards to monitor all detainees consistently and without the detainees knowing that they are constantly being watched. This concept of physical architecture was subsequently adopted by Foucault (2008) as a profound philosophical meta-

phor to describe the dynamics of pervasive surveillance and disciplinary power in modern institutions.

The panopticon concept has been applied in information systems research to capture the implications of IT's growing ubiquity and embeddedness. Poster (1995) proposed the concept of "superpanopticon" surveillance, in which data on surveillance subjects can be extracted from their phone call history, internet activity, and other technologies. As IT capabilities have grown, supervisory data can be collected from the history of actions employees perform as part of their jobs, as well as from incidental activities, such as social media engagement.

The shift from basic data gathering to this ubiquitous "superpanopticon" necessitates a reevaluation of how people perceive and respond to the risks associated with technology. While traditional TTAT focuses on risks posed by malware or system malfunctions (Boysen et al., 2019; Chen & Liang, 2019; Young et al., 2016), this study extends that theory by framing management surveillance as a deliberate, human-caused threat and creating a productivity-versus-privacy paradox. By shifting the focus from unintended technical faults to deliberate instruments, we gain a better understanding of how surveillance becomes a tool of control that employees must deal with. At the center of this response lies the Privacy Calculus (Dinev & Hart, 2006), wherein individuals engage in a cognitive analysis of potential costs and benefits. Within the confines of the panopticon, the perceived costs—including the erosion of privacy and the relinquishment of control over personal data—frequently outweigh any benefits the organization provides, thereby engendering a heightened sense of threat.

When supervision is carried out in a complex, layered, and real-time manner and the data relevant to supervision are collected from various sources, employees are likely to have a negative perception of their supervision, considering it as an activity that runs the risk of invading their privacy or at the borderline between being fit for purpose and inappropriate (Ciocchetti, 2011). Examples include monitoring text messages, GPS and RFID surveillance, IT-enabled physical surveillance, and AI-powered surveillance.

This kind of surveillance will trigger a shift in social order and values across society (Fontes et al., 2022). Employees may perceive surveillance using these technologies as scary, which can trigger their sense of threat. In addition to the fear of invasion of privacy, employees may also be concerned about getting penalized for unintentional violations of workplace rules or norms. The sanctions they may face include demotion, being assigned a job that exceeds their abilities (Callahan & Bok, 1980), elimination of benefits, job loss, and degradation of their work environment (Mesmer-Magnus & Viswesvaran, 2005).

From a psychological standpoint, this perceived threat stems from the potential loss of freedom. According to Psychological Reactance Theory (Brehm & Brehm, 1981, p. 35), when people experience psychological reactance due to surveillance restricting their behavioral freedom, they may develop a desire to regain that freedom. While this study mainly focuses on threat-avoidance intents as described by the TTAT, noting the psychological need to regain autonomy provides a core perspective for understanding employees' instinctive responses to panopticon surveillance.

Protection Effectiveness

When employees encounter IT that poses a risk, they often seek effective solutions to protect their interests. According to Liang & Xue (2010), protection effectiveness is the evaluation of measures put in place to prevent the appearance of any incoming risks. This

rating is based on the predicted outcomes when these protective measures are implemented. Traditionally, TTAT views protection as an individual cognitive process in which an individual follows protection recommendations provided by others with a better understanding of information technology (Dodge et al., 2023).

However, this study expands on TTAT by incorporating the social dimension of protection effectiveness. We argue that in a panopticon environment, where surveillance and resistance are collective, the decision to avoid surveillance extends beyond an isolated cognitive process and functions as a socially reinforced protection mechanism (Schoenherr, 2020). In this context, the perceived effectiveness of protective actions increases when they are shared or observed in peer groups, thereby transforming individual avoidance into a collective strategy (Penić et al., 2024).

Examples of protective activities that employees can perform to protect their interests and distance themselves from panoptic surveillance include not using an ID card, lowering their voice when chatting, writing criticisms on social media and the web, and sabotaging and hacking surveillance technology (Ball, 2010; Martin & Freeman, 2003). Employees assess the effectiveness of these protections and decide whether the surveillance technology can be bypassed.

Notably, an employee's capacity to analyze and apply protective measures varies; it is heavily influenced by their professional background and technical expertise (Hooper & Blunt, 2020). For instance, deploying technical countermeasures such as system evasion or sabotage requires a thorough IT architecture understanding. As a result, people with strong technical backgrounds, such as IT personnel, tend to have different appraisals of the efficacy of protections and a more optimistic outlook on appraising technology-related risks than non-IT employees. This variation in core capabilities relates to different assessments of their resistance to extensive surveillance (Fatoki et al., 2024). This comparative perspective is crucial in behavioral research for identifying how specific contextual backgrounds, such as organizational or professional environments, shape different mindsets and behavioral intentions (Cao & Ngo, 2019). Recognizing these professional distinctions is critical for understanding how different groups of employees assess their ability to withstand broad observation.

The Threat of Surveillance Technology in Panopticons and Avoidance Intention

Technology-based management control can make organizations transparent, open, traceable, and accountable entities (Brivot & Gendron, 2011; Csapo & Brisan, 2014). IT-based management control can provide qualified controls to monitor employee work activities. Their use will make employees aware that they are being watched and are constantly being seen, thereby changing their behavior (Brivot & Gendron, 2011).

IT-based management controls may improve employees' behavior but may also worsen it. The practice of supervision is perceived as excessive and is associated with negative employee behavior in three distinct circumstances (Ball, 2010): i) when supervision is deemed unreasonable, for example, supervision extends to the employee's personal life; ii) when supervision is carried out to know precisely how much time is spent by employees in the company; and iii) when supervision harms employee autonomy and trust. When supervision is carried out using simple IT, it does not lead to these three conditions, and the supervisory technology will be perceived as ordinary. Such conditions in this study

are referred to as "non-panoptic surveillance". Non-panopticon supervision will not create negative employee perceptions because it is simple and considered regular supervision.

Unlike non-panoptic surveillance, surveillance using continuous, complex, layered, and real-time IT encourages the appearance of three conditions described by Ball (2010), which is called the "panoptic surveillance" (Holt et al., 2017). Panopticon surveillance will be considered malicious because it threatens privacy, ethics, and human rights. Employee privacy and human rights are threatened because surveillance technology can monitor their activities in detail. This surveillance technology can record in detail when they leave the table and the time they spend using the telephone or cell phone. Surveillance technology is also considered a threat due to loudspeakers and voice recorders in every room, as well as the monitoring of computer logs to track employee activity. Threats can also arise from panoptic surveillance, which may interfere with employees' privacy through radio frequency identification (RFID) sensors placed at various points (Ciocchetti, 2011).

Liang & Xue (2009, 2010) state that perceived IT threats are similar to those of human health. Threats and disruptions from IT systems specifically designed for surveillance can lead to privacy violations, decreased creativity, and financial losses (Ball, 2010; Liang & Xue, 2010). Posey et al. (2011) explain that supervisory procedures that threaten or invade employee privacy will backfire on the organization. Thus, increasingly excessive supervision will intensify the perceived threat to privacy, thereby increasing individuals' motivation to avoid it. Also, increasingly intensive surveillance will lead to resistance from those affected (Munn, 2024). Resistance can take the form of identifying and exploiting weaknesses in the system, distorting data, and developing an anti-compliance attitude towards the system.

Drawing on Technology Threat Avoidance Theory (TTAT), this study argues that panopticon surveillance causes significant discomfort and technological stress, manifested in behavioral tensions such as decreased productivity and increased turnover (Cooper et al., 2001; Jex & Beehr, 1991). Although the current application of TTAT focuses on reactive avoidance of unintended threats (e.g., malware), this study develops the theory by applying it to the dynamics of intentional structural power in a panopticon environment. By presenting surveillance as not only a technical risk but also a management control mechanism, this study shifts the focus from risk mitigation to opposition to institutional transparency. This viewpoint will provide a better understanding of how control paradoxically causes widespread employee avoidance.

Thus, the first hypothesis for the study is as follows:

H1: The degree of employee avoidance intention will be higher when the surveillance is implemented in a panopticon than in a non-panopticon setting.

Protection Effectiveness and Avoidance Intention

Liang and Xue (2010) define protection effectiveness as the extent to which a security measure prevents emergent threats. Protection effectiveness reflects how much employees can control threats using various types of protection. The effectiveness of protection in the technology threat avoidance theory (TTAT) is based on expected outcomes that measure the benefits of protection implemented to avoid objectively dangerous information technology (Liang & Xue, 2009).

The effectiveness of protection in the technology threat avoidance theory (TTAT)

is based on outcome expectancy, which measures the benefits of protection undertaken to objectively avoid harmful information technology (Liang & Xue, 2009). The better the estimate of the results obtained when using existing safeguards or circumvention measures, the more likely an employee will see the protection as effective. Estimates are made based on the benefits and costs of providing security.

Forms of protective activities that need to be considered for their effectiveness when faced with a threat, including not using an ID card, not using an ID card with a barcode when leaving their work desk, lowering their voice, sabotaging supervision practices, and posting on the counter, institutional web (Ball, 2010), hacking surveillance technology (Martin & Freeman, 2003), generating distrust, and attempting to resign (WorkTime, 2019). These activities carried out by employees are a form of coping behavior aimed at avoiding problems that cause them stress (Folkman et al., 1986).

The more employees who perform these activities, the more other employees will perform the same or other actions with the same purpose. This, in turn, will increase the effectiveness felt by everyone, as Kim and Kankanhalli (2009) explained that colleagues' opinions influence the acceptance and rejection of technology implemented in the workplace. Therefore, employees will be more motivated to avoid panopticon surveillance if many of their colleagues use these activities and successfully avoid them. Simply put, the protection activities will be effective. In line with the process-based approach in management, this suggests that employees' subjective interpretations of organizational practices constitute a critical psychological process that directly shapes their behavioral intentions, such as the intention to leave the company (Tandung, 2016).

This avoidance intention reflects employees' coping assessments, in which perceived response efficacy (the effectiveness of protection) is particularly important in predicting the intention to act (Dodge et al., 2023). This response efficacy increases in line with collective actions taken by employees against surveillance. Accordingly, individuals perceive this as a social reward (rather than a compliance reward) that strengthens their motivation to engage in avoidance. This reward reinforces their perception that the protective actions taken are effective.

Thus, the second hypothesis states that:

H2: Employees' avoidance intention will be greater when the level of protection effectiveness is high than when it is low.

The Threat of Surveillance Technology in Panopticons, Protection Effectiveness, and Avoidance Intention

The relationship between the threat of panopticon surveillance and protective effectiveness can be understood as an employee's capacity to act when confronted with conflicts arising from the company's strategy (Carls, 2009). When panopticon surveillance is implemented, some areas of employee flexibility of interest will be taken over by it, with technology further increasing the supervisor's supervisory power. This occurs because sophisticated IT enables supervisors to conduct surveillance that collects and stores comprehensive data on employees' activities during working hours. Furthermore, such technology can facilitate continuous, real-time supervision (Zuboff, 1988). As employees are usually aware of such surveillance technologies in their workplaces and their capabilities, the growing use of these technologies has increased the openness and transparency of supervision (Liew,

2015) and potentially reduced human-derived bias during supervision.

At the same time, such technology-centric supervision may make employees feel their privacy is threatened (Martin & Freeman, 2003) and prompt them to seek ways to evade surveillance. As part of this threat-avoidance process, employees will assess the effectiveness of protection measures that allow them to circumvent surveillance technologies (Liang & Xue, 2010). Employees avoid technology-based threats by taking the most effective protective measures (Arachchilage & Love, 2014). However, when employees assess the effectiveness of protective measures as low, or their capacity to act is low, they will be reluctant to avoid surveillance technology. This discussion leads to the third hypothesis, which is:

H3: Employee avoidance intention in response to the panopticon surveillance is moderated by protection effectiveness, which will be greater when protection effectiveness is high than when it is low.

METHOD

Design

This study employed an internet-based experiment with a 2x2 between-subjects factorial design. The initial variable manipulated in this study is the threat of surveillance technology, which is examined by contrasting panoptic (coded as P) versus non-panoptic (N) surveillance. The second variable investigated is the effectiveness of protection against surveillance threats, with high (H) and low (L) effectiveness distinguished. Respondents in the Jakpat app—an Indonesian-based independent survey service company with a database of respondents from various backgrounds (Jakpat, 2025)—were randomly sent an instrument with two different manipulations. In particular, they were presented with one of the following manipulations: either a panopticon and high effectiveness protection (P-H), a panopticon and low effectiveness protection (P-L), a non-panopticon and high effectiveness protection (N-H), or a non-panopticon and low effectiveness protection (N-L).

Participants Study 1

Participants in Study 1 were information technology (IT) workers with at least one year of professional experience. They were selected because they were more familiar with new surveillance technologies and were expected to be more familiar with the research instrument. Only 199 of the 208 participants met the criteria of IT workers. Furthermore, 26 participants were excluded for failing to answer the manipulation check question correctly, leaving 173 for analysis. Male respondents comprised 86% (148) of the total respondents, and their average age was 30 years old.

Before the study, a pilot test was conducted on individuals with characteristics similar to those of the actual participants. The first trial was conducted with four accounting master's students at a university in Yogyakarta, Indonesia, to validate the questionnaire's manipulation and content. The second trial was conducted on 29 respondents to test whether the online media functioned properly and the experimental procedure ran smoothly. Input regarding the content of the experimental instrument to be tested was obtained from both trials.

Independent Variables

The first independent variable is the threat posed by surveillance technology, manipulated by distinguishing between panoptic and non-panoptic surveillance technologies. Panoptic surveillance in this study includes monitoring data extracted from phone call history, internet usage history, time spent during working hours, fingerprint machines, RFID, GPS, and other technologies that can be used simultaneously. Meanwhile, non-panoptic surveillance relies solely on fingerprint attendance data for employee monitoring. Manipulation for surveillance technology was adopted from Holt et al. (2017).

The second independent variable is protection effectiveness, which refers to the effectiveness of various actions performed to avoid surveillance technology. The protection actions include reporting the company for violating privacy, sabotaging surveillance practices, posting articles protesting online or on social media platforms, hacking surveillance technology, creating distrust in the company, and encouraging resignations. Protection effectiveness in this study is divided into high and low effectiveness. The report indicates high protection effectiveness, with an 80% success rate in taking action to avoid surveillance threats in these ways. Conversely, a success rate of 20% indicates low protection effectiveness. The manipulation of protection effectiveness was developed using Chen & Liang's (2019) instrument.

Dependent Variables

The dependent variable in this study is avoidance intention. In compliance with Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009), this study measures avoidance intention as the dependent variable by analyzing the questionnaire answers given to respondents. The measurement scale for the dependent variable was adapted from Liang & Xue (2010) using a 7-point Likert scale from 1 (strongly disagree) to 7 (strongly agree). The dependent variable score was calculated by averaging the scores for the five statements given. A high mean indicates that participants tend to have the intent to avoid supervision, while a low one indicates the opposite.

Pearson Correlation testing was used to test the validity of the constructs. The results for 22 respondents (7 of 29 pilot respondents did not pass the manipulation check) showed a significant p-value ($p < 0.01$) and a calculated R-value above the R table value of 0.537 ($n=22$, $df=20$). Furthermore, Cronbach's alpha was used to assess reliability, yielding a value of 0.944, exceeding the 0.7 threshold. Overall, the constructs in this study have good validity and reliability.

Task and Procedures

Participants in this experiment were obtained using the Jakpat app. Jakpat's database is similar to the online labor market, which, according to Horton et al. (2011), provides a diverse pool of workers for conducting experiments and has great potential to support laboratory research.

Jakpat app users who meet the criteria as participants in this study are randomly sent a case containing a manipulation treatment. Each respondent will receive only one condition and cannot choose or see any others. At the beginning, each participant is given a pre-treatment question to eliminate those who do not meet the criteria, ensuring the experiment's randomization is correct. Participants are then asked to complete the task as instructed. Participants will then complete two manipulation check questions to ensure

they understand the case provided.

All participants received a case explaining that they are employees of PT Sarana Global Computer and that the company has implemented an employee surveillance technology. Each participant is assigned to one of four different experimental conditions: Condition 1: panoptic surveillance technology and high protection effectiveness (PH), which is a case with panoptic surveillance and high protection effectiveness (80%); Condition 2: panoptic surveillance technology and low protection effectiveness (PL), which is the case with panoptic surveillance and low protection effectiveness (20%); Condition 3: non-panoptic surveillance technology and high protection effectiveness (NH), which is the case with non-panoptic surveillance and high protection effectiveness (80%); or Condition 4: non-panoptic surveillance technology and low protection effectiveness (NT), which is the case with non-panoptic surveillance and low protection effectiveness (20%). Details of the four manipulations are as follows (Figure 1):

Variable/Manipulation		**Protection Effectiveness**	
		High	Low
The threat of surveillance technology	Panopticon	**Condition 1** (Panopticon surveillance – High protection effectiveness)	**Condition 2** (Panopticon surveillance – Low protection effectiveness)
	Non-panopticon	**Condition 3** (Non-panopticon surveillance – High protection effectiveness)	**Condition 4** (Non-panopticon surveillance – Low protection effectiveness)

Figure 1. Manipulation for each condition in Study 1

Statistical analysis

Hypothesis testing was performed using two-way ANOVA. ANOVA was selected for the 2x2 factorial experimental design, which aimed at comparing mean differences across distinct treatment groups. ANOVA remains an effective standard for experimental research because it isolates the causal impact of manipulated variables and their interactions.

RESULTS

Manipulation Check Study 1

To ensure each participant understood the manipulation given, a manipulation check was conducted by asking two questions at the end of the assignment session. The first question is, "Based on the information provided at the beginning of the case (in the case explanation section), what kind of surveillance technology is applied at PT Sarana Global Computer?". The second one is, "Based on the information provided at the beginning of the case (in the case explanation section), what is the effectiveness percentage of the methods that circumvent surveillance technology?".

One hundred ninety-nine participants who correctly answered the pre-question

were randomly assigned to four manipulation conditions. In the first manipulation (P-H), 86% (44 of 51) answered the check-manipulation questions correctly. Similarly, in the second manipulation (P-L), 81% (42 of 52) answered correctly. In the third manipulation (N-H), 88% (44 of 50) answered correctly, and in the fourth manipulation (N-L), 78% (43 of 55) answered correctly. In total, 173 participants answered both questions correctly.

Descriptive Statistic Study 1

Table 1 shows that the average age of participants is 30.06 years ($\sigma = 6.64$). The youngest participant is 18, and the oldest is 49. Most respondents are male (85.5%). The shortest and longest working periods are 2 and 4 years, respectively, with an average of 3.02 ($\sigma = 0.88$). Bachelor's degree (57.8%), high school (31.2%), a 3-year diploma (4%), master's degree (3.5%), junior high school (1.7%), 1-year diploma (1.2%), and elementary school (0.6%).

Table 1. Descriptive Statistics Study 1

Variable	N	Minimum	Maximum	Mean	SD
Age	173	18	49	30.06	6.647
Working Period	173	2	4	3.02	0.882

To ensure adequate randomization, examinations were conducted for each demographic information, including age group, gender, length of service, and education level. Results showed no differences among age (χ^2=0.403, df=180, p>0.05), gender (χ^2=0.202, df=30, p>0.05), working period (χ^2=0.059, df=60, p>0.05), and education level (χ^2=0.991, df=180, p>0.05), based on the assignment. This result indicates that the randomization was effective.

Hypothesis Testing

The first hypothesis in this study predicts that employee avoidance intention will be higher when supervision is panopticon than when it is non-panopticon. The ANOVA hypothesis test presented in Table 2 shows p<0.05 (F = 52.2). It indicates that panopticon supervision influences employee avoidance intention. This influence is evidenced by the higher average score for employee avoidance intention when the supervision is panopticon supervision (24.81) than when it is non-panopticon (16.12), as shown in Table 3. Therefore, this finding supports the first hypothesis in Study 1.

Table 2. ANOVA Test Results Study 1

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	3514.007[a]	3	1171.336	18.862	0.000
Intercept	72308.940	1	72308.940	1164.415	0.000
Surveillance	3241.562	1	3241.562	52.200	0.000
Protection	216.952	1	216.952	3.494	0.063
Surveillance * Protection	33.978	1	33.978	0.547	0.461
Error	10494.722	169	62.099		
Total	86323.000	173			
Corrected Total	14008.728	172			

a. R Squared = .251 (Adjusted R Squared = .238)

Table 3. Descriptive Statistics Results on Avoidance Intention Dependent Variables

Variables	Manipulations	N	Mean	SD
Surveillance	Panopticon	86	24.814	8.081
Technology Threats	Non-Panopticon	87	16.126	4.271
Protection	High	88	21.658	9.433
Effectiveness	Low	85	19.282	8.481

The second hypothesis predicted that employee avoidance intention would be higher when protection effectiveness is high than when it is low. Table 2 presents a value of p=0.063 (F=3.49), indicating a weak effect of protection effectiveness on avoidance intention. The mean also shows this in Table 3, with a higher score for high effectiveness (21.65) than for low effectiveness (19.28). Therefore, it can be concluded that H2 is not supported in Study 1.

H3 predicts that the effectiveness of protection will moderate employee avoidance intention when panopticon surveillance is applied. Meaning to say, when organizations implement panoptic surveillance technology, employees with high protection effectiveness will have greater avoidance intention than those with low protection effectiveness. Table 2 shows p=0.46 (F=0.547), indicating that the variable does not moderate the causal relationship. Thus, the third hypothesis in Study 1 is not supported.

In evaluating the fit of the model presented in Table 2, the analysis yielded an Adjusted R^2 value of 0.238, indicating that the independent variables explain 23.8% of the variance in employee avoidance intention. Although this explanatory power is regarded as moderate, it is consistent with an experimental strategy that prioritizes theoretical simplicity (Ozili, 2023). This is because the study focuses on isolating the specific impacts of panopticon manipulation rather than accounting for all possible determinants of avoidance intentions. This value provides a solid and appropriate basis for assessing the hypothesized causal link.

DISCUSSION

The results of the first hypothesis show that panopticon surveillance significantly increases employee avoidance intentions relative to non-panopticon surveillance. These findings are consistent with the threat assessment in TTAT, indicating that employees perceive panopticon surveillance as a potential threat to their privacy and autonomy (Liang & Xue, 2009). In contrast to traditional surveillance, the everlasting visibility inherent in the panopticon creates a condition of continuous active surveillance, hence eroding organizational trust and employees' ethical perceptions (Holt et al., 2017). As a result, employees' drive to avoid the system serves as a response to both surveillance and the perceived systemic threat.

These findings provide empirical support for the Big Brother metaphor, which holds that persistent digital surveillance produces a perceived power imbalance (Power, 2016). In this study, avoidance intention was manifested as blinking back: a method used by a group of employees to defend themselves from the unwavering panoptic gaze. While panopticon monitoring aims for absolute and continuous visibility, blinking back is a coping technique for regaining a sense of privacy and autonomy in a heavily monitored setting.

In contrast to Liang & Xue's (2009, 2010) conceptualization of threats in the use of active technology (such as malware), our findings demonstrate that intrusive technology—integrated into an organization's infrastructure—elicits analogous defensive motivations. Specifically, this study extends the Threat Threat Avoidance Theory (TTAT) by elucidating that threat avoidance can be initiated by institutional technology that does not necessitate direct user interaction. This refines the theory by shifting the focus from user-technology interaction to the implementation of institutional technology (Potts et al., 2025). This underscores the inherent, non-negotiable nature of panopticon surveillance, making it a stronger predictor of avoidance intentions than interactive threats.

The second hypothesis yielded a marginal trend indicating a protective effect on employee avoidance intention, but it did not reach statistical significance. Although H2 is not supported, the observed impact direction is consistent with the coping evaluation process in the TTAT framework, notably the function of response effectiveness. This suggestive pattern shows that the perceived efficiency of protective interventions significantly motivates avoidance intention, albeit not as strongly as the actual threat itself. In theory, this means that when employees believe specific countermeasures are effective in decreasing the threat of monitoring, they are more likely to participate in increases (Carpenter et al., 2019; Liang & Xue, 2010). This suggests a rationalized response in which individuals do not merely react impulsively to surveillance but instead attempt to assess the feasibility of their countermeasures (Chen & Zahedi, 2016).

Although the statistical evidence is inconclusive, the findings indicate that effective mitigation strategies can help employees regain their privacy and autonomy (Young et al., 2016). (Ásványi, 2022) emphasizes the importance of properly selecting control devices to protect employee privacy and rights. The implications of these findings suggest that theoretical advances in protection efficacy may not be limited to institutional instruments but may potentially include strategies devised and adopted independently by employees. Even without strong statistical significance, this trend suggests that, in the face of invasive managerial controls, employees may shift from passive subjects to active agents who strategically consider self- and group-initiated protection (Taylor & Dobbins, 2021). Thus, although not a primary determinant in this study, the effectiveness of coping measures remains a factor worthy of further exploration in the context of invasive surveillance.

The results for the third hypothesis show that the interaction between the perceived threat of panopticon surveillance and protection effectiveness is not supported. That is to say, although the supervision variable affects the dependent variable, and the protection effectiveness variable affects it moderately, the protection effectiveness (high-low) does not affect the causal relationship between panopticon supervision and avoidance intention. From a theoretical perspective, this unexpected result prompts a further theoretical review of the internal dynamics of the TTAT framework, in which the phenomenon of threat appraisal dominance emerges as an interpretive explanation for understanding these findings (Liang & Xue, 2010). When faced with panoptic surveillance—one perceived as an extreme and invasive threat to privacy—the motivation to avoid the threat becomes so overwhelming that it bypasses the evaluation of coping effectiveness. In such high-pressure environments, employees prioritize reclaiming their autonomy through avoidance regardless of whether their protective measures are technically superior or limited (Lowry & Moody, 2015).

This study proposes that employees' behavior in avoiding panoptic surveillance technology is not influenced by the effectiveness of existing protective measures, but rath-

er by the inherent nature of the threat itself. These findings imply that organizational decisions regarding the adoption of control tools should reflect not only technical issues but also the psychological impact of surveillance (Junqueira et al., 2016). According to Psychological Reactance Theory (Brehm & Brehm, 1981, p. 60), severe surveillance can elicit an innate desire to fight perceived risks or loss of freedom, independent of the perceived effectiveness of defensive measures. By integrating this theory, we manage to see it as a fundamental response to perceived loss of freedom (Graupmann et al., 2016; Rosenberg & Siegel, 2018). In this case, the threat of surveillance to employees' privacy and rights is a better predictor of avoidance than technical achievement metrics. This reframes the study's contribution by demonstrating that when surveillance reaches a panoptic scale in institutional settings, the typical balance between threat assessment and coping appraisal shifts toward a sole, overwhelming focus on threat avoidance.

Since the use of Psychological Reactance Theory is intended as a retrospective attempt to explain the lack of statistical significance in H3, we present this finding as an exploratory idea for future empirical testing. This idea provides a crucial theoretical bridge, suggesting that a psychological need to blink can override rational assessments of safety precautions in high-pressure monitoring contexts; further thorough deductive inquiry is required to confirm.

STUDY 2

To more firmly integrate findings of Study 1 and explore the boundary conditions of the TTAT framework within an institutional setting, we conducted Study 2. This study was conducted by testing and comparing the experimental instrument from Study 1 with respondents from non-IT professional backgrounds. This study was conducted to explore how IT and non-IT employees' technological skills and understanding affect their perceptions. Previous research has found differences in the most important work values between IT and non-IT employees (Toskin & McCarthy, 2019).

IT employees seek more meaningful, challenging, and thought-provoking work than non-IT employees. Regarding supervision with advanced technology, employees with non-IT backgrounds may feel disturbed by a mismatch between their abilities, knowledge, and personal values and the company's supervision culture (Zhang et al., 2012). In the digital era, employees with opportunities, motivation, and rationalization are unlikely to commit fraud when they lack the capability to use digital platforms (Othman & Ameer, 2022).

Study 2 involved respondents with financial backgrounds who worked in the finance department at a university in Yogyakarta, Indonesia. Study 2 uses financial staff for non-IT participants because the wage differential between financial-sector workers and others is greater (Luo & Zhu, 2014; Sum et al., 2008). Data from the Indonesian Central Bureau of Statistics show that the financial sector ranks first in wage receipts, while the information and communication sector ranks fourth (BPS, 2024).

This reason is based on previous research that concluded that salary affects employee job satisfaction (Hasin & Omar, 2007; Kothalawala & Samarakoon, 2018). Another reason for using finance staff is that the financial sector, particularly accounting and auditing in public accounting firms, is identified as a highly stressful area of specialization. This ultimately results in performance issues and a subsequent intention to leave the organiza-

tion (Hasin & Omar, 2007).

The Study 2 sample comprised 74 participants, but only 65 (87.8%) were included in the analysis because 9 participants failed the manipulation check. Fifteen participants were in the first manipulation (P-H), 19 participants were in the second manipulation (P-L), 13 participants were in the third manipulation (N-H), and 18 participants were in the fourth manipulation (N-L). Figure 2 summarizes the distribution of samples for each manipulation. The majority of the participants were female (60%). Forty-three participants had a bachelor's degree (66%), a 3-year diploma (20%), a master's degree (11%), and a high school degree (3%).

Treatments/Manipulation		**Protection Effectiveness**	
		High	Low
The threat of surveillance technology	Panopticon	**Condition 1 (P-H)** (Panopticon surveillance – High protection effectiveness) n = 15	**Condition 2 (P-L)** (Panopticon surveillance - Low protection effectiveness) n = 19
	Nonpanopticon	**Condition 3 (N-H)** (Non-panopticon surveillance – High protection effectiveness) n = 13	**Condition 4 (N-L)** (Non-panopticon surveillance - Low protection effectiveness) n = 18

Figure 2. Manipulation for each condition in Study 2

Randomization testing was also performed for each demographic. The results demonstrated that the randomization was adequate, indicating there was no difference between the age (χ^2=0.943, df=483, p>0.05), gender (χ^2=0.238, df=21, p>0.05), working period or tenure (χ^2=0.523, df=441, p>0.05), and education level (χ^2=0.529, df=63, p>0.05).

Study 2 also tested the hypothesis using ANOVA, which showed a statistically significant difference (F = 17.3, p < 0.05), as presented in Table 4. The results also indicate a tendency for financial staff to evade when confronted with supervisory pressure. This result is corroborated by the higher mean score for avoidance intention in the panopticon condition (19.64), as evident in Table 5, compared to the non-panopticon condition (10.6). Therefore, H1 is supported.

Table 4. ANOVA Test Results for Study 2

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1404.517[a]	3	468.172	6.704	.001
Intercept	14561.961	1	14561.961	208.515	.000
Surveillance	1210.315	1	1210.315	17.331	.000
Effectiveness	.910	1	.910	.013	.909
Surveillance * Effec-tiveness	79.063	1	79.063	1.132	.292
Error	4260.036	61	69.837		
Total	20957.000	65			
Corrected Total	5664.554	64			

a. R Squared = .248 (Adjusted R Squared = .211)

Table 5. Descriptive Statistics Results on Avoidance Intention Dependent Variables

Variables	Manipulations	N	Mean	SD
Surveillance	Panopticon	34	19.6471	8.97431
Tech-nology Threats	Non-Panopticon	31	10.6129	7.49078
Protection	High	28	15.2500	8.83019
Effectiveness	Low	37	15.4054	9.94278

H2 test results involving finance staff participants are presented in Table 4. They indicate no statistically significant correlation between protection effectiveness and avoidance intention (F=0.013, p=0.909). Although the mean scores in Table 5 is nearly identical (High: 15.2; Low: 15.4), this non-significant finding should be interpreted with caution. Given the small sample sizes in each cell, the analysis may lack the statistical power to detect smaller effect sizes, potentially leading to a Type II error.

The interaction effect for respondents in the finance field was also found to be insignificant (F=1.132, p=0.292). Although these results are consistent with the trend observed in Study 1, the small sample size in Study 2 reduces the statistical power available to detect interactions. Thus, although H3 is not statistically supported in this group, the small sample size in each condition may mask interaction effects that could be observed in a larger sample with higher statistical power.

Interestingly, despite the limited cell sizes, H1 in the finance group yielded a significant result ($p<0.05$, F=17.3). This suggests that the main effect of panoptic surveillance on avoidance intention is strong enough to be detected even in a limited sample. In contrast, the interaction effect (H3) may require a larger sample size.

After these results, t-tests were performed to better understand the differences. The t-test results in Table 6 were significant (t=4.02, df=245, $p<0.05$); there are differences in perceived threat avoidance across the two groups of respondents (Study 1 and Study 2). Employees with IT background are more likely to shy away from panoptic surveillance technology compared to those with finance background. This avoidance intention escalates when the protection provided is effective.

The first possible reason for this difference in the results is that employees with an IT background have greater intrinsic motivation than non-IT workers (Thatcher et al., 2006; Toskin & McCarthy, 2019). Thatcher et al. (2006) explained that intrinsic motivation, influenced by employee autonomy, ability variation, and supervisory satisfaction, will indirectly affect IT employees' intention to leave the company. Thus, in the context of this study, when IT workers are faced with an uncomfortable level of surveillance, they may decide to change jobs to avoid panoptic supervision—unlike financial employees who may choose to stay and adapt to the new surveillance climate.

Table 6. Independent Sample t-test

		t-test for Equality of Means				
		t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Different Test of Avoidance Intention	**Equal variances assumed**	4.023	245	0.000	5.067	1.260
	Equal variances not assumed	3.997	136.114	0.000	5.067	1.268

In addition to professional background, the observed variations in avoidance intention may be influenced by other factors associated with organizational sector. Individuals from the financial sector originate from public-sector universities, which are frequently characterized by enhanced job stability and risk-averse culture (Bellante & Link, 1981; Buurman et al., 2012). On the other hand, respondents from the IT sector represent a variety of private-sector businesses where monitoring systems are both obtrusive and flexible, and a performance-driven work atmosphere is more prevalent.

Although this dual difference (IT/Private Sector vs. Finance/Public Sector) adds complexity, we believe it effectively represents the regulatory landscape. In the public sector, job security may reduce the temptation to deliberately evade or engage in evasion since employees may prioritize long-term stability over privacy concerns. Conversely, increased evasion among IT/private-sector professionals is likely roots from a combination of great technological proficiency and a low tolerance for technologies that limit their autonomy. As a result, the outcomes of this study should be viewed as a reflection of professional knowledge and the socio-technical environment in which people work.

Furthermore, differences in avoidance intention can be ascribed to variations in technological self-efficacy and domain-specific expertise. In contrast to IT professionals, financial professionals may experience a significant gap in their understanding of the core mechanisms of panoptic surveillance (Zhang et al., 2012). This lack of technical proficiency is commonly manifested as technophobia (Firk et al., 2024), in which the focus turns from avoiding hazards to just tolerating the deployment of unfamiliar work practices. From a TTAT standpoint, whereas IT experts have the necessary security knowledge to evade and prevent surveillance, financial staff may be overwhelmed by the complexities of the systems, hence leading to passive compliance rather than proactive evasion.

These results have implications for control practices in an organization, especially because they provide evidence that the same type of surveillance technology can affect the perceptions and behavior of two groups with different characteristics. Tomczak et al. (2018) explain that electronic surveillance systems should be tailored to each organization. Employees with IT and other professional backgrounds have different job characteristics and tasks. Compared to employees from other backgrounds, IT employees who prioritize freedom and autonomy in their work need a more flexible supervisory system (Thatcher et al., 2006; Tomczak et al., 2018).

CONCLUSIONS

This study develops the Theory of Technological Threat Avoidance (TTAT) by demonstrating that panoptic surveillance functions as a powerful institutional threat triggering sophisticated avoidance intention. Our findings provide robust support for the primary effect (H1), confirming that panoptic monitoring elicits significantly higher levels of resistance than non-panoptic controls due to the lesser ethical commitment among employees to the company (Holt et al., 2017). These findings support expanding TTAT's traditional focus on external technical risks into the realm of internal management control systems. However, the main effects on protection effectiveness and the interaction between threat and protection effectiveness were statistically insignificant. This demonstrates the ubiquitous influence of threat evaluations in panopticon surveillance settings. Notably, the perceived threat posed by invasive systems is so great that it significantly outweighs rea-

sonable assessments of countermeasure effectiveness, goes beyond organizational ethical standards, and transcends specialized professional backgrounds. This is a psychological reaction that leads to basic resistance, often overlooking technical considerations regarding the likely success of countermeasures.

This study makes two contributions to the literature. The study's findings shed light on the practical and societal ramifications of deploying technology surveillance, highlighting the importance of properly selecting control measures. Aside from operational efficiency, the priority should be on employees' psychological well-being, privacy rights, and trust. Panoptic surveillance occurs in an increasingly stringent worldwide regulatory environment, and its deployment is not unique. Frameworks such as the European Union's General Data Protection Regulation (GDPR) require workplace monitoring to adhere to the principles of proportionality and data minimization. Invasive monitoring that disregards these boundaries is no longer just an internal policy blunder; it is a breach of fundamental human rights with serious legal and societal ramifications.

When organizations fail to follow ethical and regulatory guidelines, the consequences for employees can be disastrous. As previously reported, the adoption of severe surveillance fundamentally affects the psychological contract, resulting in undesirable outcomes such as increased stress, job dissatisfaction, impression of being overused, and emotional exhaustion (Noreen et al., 2021). However, possible conflicts resulting from the incorrect use of monitoring techniques are frequently underestimated (Chenhall & Moers, 2015). To reduce these risks, managers could consider digitalizing management control in accordance with current privacy standards (Abernathy et al., 2019). Overreliance on panoptic control instruments, along with a lack of open communication, results in a systemic loss of organizational confidence. When confidence is eroded, employees shift from collaborative stakeholders to defensive actors, threatening the organization's long-term stability and effectiveness (Christ, 2013).

This study broadens the scope of the TTAT by shifting the threat area from external technical risks to internal institutional technology threats under management control. While TTAT is often used to address external threats, our findings show that it can also be applied to organizational monitoring when the institution itself becomes a threat. This study identifies the predominance of threat assessment, demonstrating that in extremely intrusive panoptic conditions, the perceived threat to privacy becomes so overwhelming that it overshadows the appraisal of countermeasure performance. This proposes a hierarchy within TTAT elements, in which traditional linear correlations between danger and coping appraisals are disturbed as monitoring scales up.

Furthermore, this study demonstrates that the relationship between employers and employees is stretched not only by technology but also by breaches of professional autonomy, with occupational background functioning as an important boundary condition for TTAT. According to Goebel & Weißenberger (2017), strengthening control mechanisms does not always increase control; our empirical evidence suggests that digitalization can lead to significant employee unhappiness and poor organizational influence outcomes (Chenhall & Moers, 2015; Mulvaney, 2019). While practical implications suggest that managers would benefit from communicating openly to bridge information gaps (Malmi & Brown, 2008), the primary theoretical contribution lies in framing avoidance intention as a fundamental psychological defense of privacy that transcends the technical efficacy of control instruments.

LIMITATIONS AND FUTURE STUDIES

There are some limitations to this study. Firstly, it should be noted that this study does not discuss the distinguished features between human-operated and fully automated surveillance technology. As a matter of fact, it focuses on the distinction between surveillance with multiple technologies and surveillance with a single technology. As Raveendhran & Fast (2021) explain, people tend to accept tracking technology in organizations when it is implemented automatically without human intervention. This is because subjective judgment is possible when human intervention is involved. This distinction will be crucial to investigate further in future studies, focusing on the performance, trust, and well-being of individuals within the organization concerning implementing human-operated and fully automated surveillance technologies.

Secondly, the proposed hypothesis does not address the potential influence of psychological factors on employees' decisions to take avoidance actions. Consequently, further research is required to incorporate either independent or moderate psychological variables. In particular, when panopticon-like surveillance is implemented, it is essential to understand how employees are willing to accept it.

Thirdly, the present study was limited to Jakpat users who met the specified criteria and came from diverse organizations. This may affect how they perceive the threat posed by surveillance technology. In future studies, we recommend investigating our findings in the context of real-world tasks and situations with participants under the same organization. This could be achieved through longitudinal research, enabling the measurement of real employee behavior.

Fourthly, the sample size for each cell in Study 2 involving finance staff is relatively small. This reduction in statistical power increases the risk of error, particularly regarding interaction effects. Future research is advised to use a larger sample across various occupational sectors to confirm whether interactions between the type of supervision and the effectiveness of protections are indeed absent among non-IT staff.

Finally, there are methodological considerations to note regarding our experimental design. To ensure that strong internal validity and a clear causal contrast are achieved, the non-panopticon condition was created using only attendance monitoring via fingerprint machines. While this maximizes internal validity, it sacrifices some ecological validity. This is because, in practice, most organizations have implemented a moderate level of electronic surveillance, rather than no monitoring at all. As a result, this pronounced distinction may have contributed to an overestimation of the observed effect size.

Because this work specifically focused on causal links, more advanced analytical tools, such as Structural Equation Modeling (SEM), could be used in future research. SEM could be used to broaden the existing paradigm as it helps examine multi-layered mediation paths—such as the role of perceived organizational justice or psychological reactance—that were not included in the core causal research.

Furthermore, while our quantitative results are strong, we recognize that a mixed-methods approach could enhance the findings. Subsequent research could include qualitative components, such as in-depth interviews, to highlight nuanced contextual elements and distinctive employee coping techniques that a standardized experimental instrument may not fully capture. This would provide a more specific "lived experience" of digital panopticism in various organizational settings.

Statements and Declarations:
This work was supported by Program Rekognisi Tugas Akhir 2020 from Direktorat Penelitian Universitas Gadjah Mada (Grant Number: 2607/UN1/DITLIT/DIT-LIT/PT/2020). The authors have no competing interests to declare that are relevant to the content of this article.

REFERENCES

Abernathy, J. L., Beyer, B., Downes, J. F., & Rapley, E. T. (2019). High-Quality Information Technology and Capital Investment Decisions. *Journal of Information Systems.*

Aldianto, L., Tjakraatmadja, J. H., Larso, D., Primiana, I., & Anggadwita, G. (2021). A technological innovativeness measurement framework: A case study of technology based Indonesian companies. *Gadjah Mada International Journal of Business, 23*(1), 91–112.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.

Ásványi, Z. (2022). Technology vs privacy at work: The extent and limitations of organizational control mechanisms. *Management: Journal of Contemporary Management Issues, 27*(2), 261–282.

Azmy, A. (2024). Employee satisfaction factors in the e-commerce company: the mediating role of employee engagement. *Journal of Indonesian Economy and Business, 39*(1), 28–56.

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

Bao, Y., Li, W., Ye, Y., & Zhang, Q. (2022). Ethical Disputes of AI Surveillance: Case Study of Amazon. *2022 7th International Conference on Financial Innovation and Economic Development* (ICFIED 2022), 1339–1343.

Bellante, D., & Link, A. N. (1981). Are public sector workers more risk averse than private sector workers? *ILR Review, 34*(3), 408–412.

Bentham, J. (1791). *Panopticon, Or the Inspection-house: Containing the Idea of a New Principe of Construction Applicable to Any Sort of Establishment in Wich Persons of Any Description are be Rept Under Inspection...* By T. Payne.

Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the threat calculus of technology threat avoidance theory. *Communications of the Association for Information Systems, 45*(1), 5.

BPS. (2024). *Rata-Rata Upah/Gaji - Tabel Statistik - Badan Pusat Statistik Indonesia.* Badan Pusat Statistik. https://www.bps.go.id/id/statistics-table/2/MTUyMSMy/rata-rata-upah-gaji--rupiah-.html

Brehm, S. S., & Brehm, J. W. (1981). *Psychological reactance: A theory of freedom and control.* Academic press.

Brivot, M., & Gendron, Y. (2011). Beyond panopticism: On the ramifications of surveillance in a contemporary professional setting. *Accounting, Organizations and Society, 36*(3), 135–155.

Buurman, M., Delfgaauw, J., Dur, R., & Van den Bossche, S. (2012). Public sector employees: Risk averse and altruistic? *Journal of Economic Behavior & Organization, 83*(3), 279–291.

Callahan, D., & Bok, S. (1980). *Ethics Teaching in Higher Education* (1st ed.). Plenum Press.

Cao, V. Q., & Ngo, T. T. T. (2019). Linking entrepreneurial intentions and mindset models:

A comparative study of public and private universities in Vietnam. *Gadjah Mada International Journal of Business, 21*(2), 115–133.

Carls, K. (2009). Coping with control? Retail employee responses to flexibilisation. *Qualitative Research in Accounting & Management, 6*(1/2), 83–101.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*(1), 380–407.

Charbonneau, É., & Doberstein, C. (2020). An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector. *Public Administration Review, 80*(5), 780–791. https://doi.org/10.1111/PUAR.13278

Chen, D. Q., & Liang, H. (2019). Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory. *IEEE Transactions on Engineering Management, 66*(4), 552–567.

Chen, Y., & Zahedi, F. M. (2016). Individuals'internet security perceptions and behaviors: polycontextual contrasts between the united states and china. *MIS Quarterly, 40*(1), 205–222.

Chenhall, R. H., & Moers, F. (2015). The role of innovation in the evolution of management accounting and its integration into management control. *Accounting, Organizations and Society, 47*, 1–13.

Christ, M. H. (2013). An experimental investigation of the interactions among intentions, reciprocity, and control. *Journal of Management Accounting Research, 25*(1), 169–197.

Ciocchetti, C. A. (2011). The eavesdropping employer: a twenty-first century framework for employee monitoring. *American Business Law Journal, 48*(2), 285–369.

Cooper, C. L., Dewe, P., & O'Driscoll, M. P. (2001). *Organizational stress: A review and critique of theory, research, and applications.*

Csapo, J. L., & Brisan, C. (2014). Aspects Concerning New Trend in Management Control Systems Design and Implementation Strategy. *Applied Mechanics and Materials, 659*, 595–600–595–600.

Dawood, S. (2023, February 13). *Amazon's worker surveillance tech "leads to extreme stress and anxiety" - New Statesman.* The New Statesman. https://www.newstatesman.com/spotlight/tech-regulation/cybersecurity/2023/02/amazon-workers-staff-surveillance-extreme-stress-anxiety

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214–233. https://doi.org/10.1016/J.JSIS.2007.09.002

Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*(4), 849–868.

Fähndrich, J. (2023). A literature review on the impact of digitalisation on management control. *Journal of Management Control, 34*(1), 9–65.

Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security, 141*, 103812. https://doi.org/https://doi.org/10.1016/j.cose.2024.103812

Fernback, J. (2013). Sousveillance: Communities of resistance to the surveillance environment. *Telematics and Informatics, 30*(1), 11–21.

Firk, S., Gehrke, Y., & Wolff, M. (2024). Digital anxiety in the finance function: Consequences and mitigating factors. *Journal of Management Accounting Research, 36*(1), 1–24.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., & Gruen, R. J. (1986). Dynamics of a stressful encounter: cognitive appraisal, coping, and encounter outcomes. *Journal of Personality and Social Psychology, 50*(5), 992.

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society, 71*, 102137.

Foucault, M. (2008). "Panopticism" from Discipline & Punish: The Birth of the Prison. *Race/Ethnicity: Multidisciplinary Global Contexts, 2*(1), 1–12.

Galliers, R. D., Newell, S., Shanks, G., & Topi, H. (2017). Datification and its human, organizational and societal effects: The strategic opportunities and challenges of algorithmic decision-making. *Journal of Strategic Information Systems, 26*(3), 185–190. https://doi.org/10.1016/J.JSIS.2017.08.002

Goebel, S., & Weißenberger, B. E. (2017). Effects of management control mechanisms: Towards a more comprehensive analysis. *Journal of Business Economics, 87*(2), 185–219.

Graupmann, V., Fryer, J. W., & Frey, D. (2016). Threat to Freedom and the Detrimental Effect of Avoidance Goal Frames: Reactance as a Mediating Variable. *Frontiers in Psychology, 7,* 632.

Haji Hasin, H., & Haji Omar, N. (2007). An Empirical Study on Job Satisfaction, Job-Related Stress and Intention to Leave Among Audit Staff in Public Accounting Firms in Melaka. *Journal of Financial Reporting and Accounting, 5*(1), 21–39.

Hartman, L. P. (1998). Ethics: The Rights and Wrongs of Workplace Snooping. *Journal of Business Strategy, 19*(3), 16–19.

Holt, M., Lang, B., & Sutton, S. G. (2017). Potential employees' ethical perceptions of active monitoring: The dark side of data analytics. *Journal of Information Systems, 31*(2), 107–124.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862–874.

Horton, J. J., Rand, D. G., & Zeckhauser, R. J. (2011). The online laboratory: Conducting experiments in a real labor market. In *Experimental Economics* (Vol. 14, Number 3).

Jakpat. (2025). *About Us.* https://jakpat.net/info/category/about-us/#:~:text=JAKPAT%20adalah%20platform%20mobile%20survei,17%2C000%2B%20followers%20di%20instagram.%20…

Jex, S. M., & Beehr, T. A. (1991). Emerging theoretical and methodological issues in the study of work-related stress. *Research in Personnel and Human Resources Management, 9*(31), l–365.

Junqueira, E., Dutra, E. V., Zanquetto Filho, H., & Gonzaga, R. P. (2016). The effect of strategic choices and management control systems on organizational performance. *Revista Contabilidade & Finanças, 27*(72), 334–348.

Kensbock, J. M., & Stöckmann, C. (2021). "Big brother is watching you": surveillance via technology undermines employees' learning and voice behavior during dig-

ital transformation. *Journal of Business Economics, 91*(4), 565–594. https://doi.org/10.1007/S11573-020-01012-X/FIGURES/2

Kim, H.-W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly,* 567–582.

Kothalawala, C. G., & Samarakoon, S. (2018). Job satisfaction and intention to leave: A study of financial and internal audit executive staff of public universities in Sri Lan- ka. *Kelaniya Journal of Human Resource Management, 13*(1), 49–60.

Leclercq-Vandelannoitte, A. (2019). Is Employee Technological "Ill-Being" Missing from Corporate Responsibility? The Foucauldian Ethics of Ubiquitous IT Uses in Organizations. *Journal of Business Ethics, 160*(2), 339–361.

Leclercq-Vandelannoitte, A., Isaac, H., & Kalika, M. (2014). Mobile information systems and organisational control: Beyond the panopticon metaphor? *European Journal of Information Systems, 23*(5), 543–557.

Lemieux, F. (2018). Intelligence and Surveillance Technologies. *Intelligence and State Surveillance in Modern Societies,* 165–190. https://doi.org/10.1108/978-1-78769-171-120181008

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.

Liew, A. (2015). The use of technology-structured management controls : changes in senior management ' s decision-making behaviours. *International Journal of Accounting Information Systems, 17,* 37–64.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433–463.

Luo, Y., & Zhu, F. (2014). Financialization of the economy and income inequality in China. *Economic and Political Studies, 2*(2), 46–66.

Martin, K., & Freeman, R. E. (2003). Some Problems with Employee Monitoring. *Journal of Business Ethics, 43*, 353–361.

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics, 62*(3), 277–297.

Mulvaney, M. A. (2019). Examining the role of employee participation, supervisor trust, and appraisal reactions for a pay-for-performance appraisal system. *Public Organization Review, 19*(2), 201–225.

Munn, L. (2024). Expansive and Invasive: Mapping the "Bossware" Used to Monitor Workers. *Surveillance & Society, 22*(2), 104–119.

Noreen, S., Nisar, Q. A., Haider, S., & Yean, T. F. (2021). Role of leaders' emotional labor toward leader's job satisfaction and emotional exhaustion: Moderating role of psychological capital. *Gadjah Mada International Journal of Business, 23*(1), 36–54.

Othman, R., & Ameer, R. (2022). In employees we Trust: Employee fraud in small businesses. *Journal of Management Control, 33*(2), 189–213. https://doi.org/10.1007/s00187-022-00335-w

Ozili, P. K. (2023). The acceptable R-square in empirical modelling for social science research. In *Social research methodology and publishing results: A guide to non-native*

English speakers (pp. 134–143). IGI Global Scientific Publishing.

Penić, S., Donnay, K., Bhavnani, R., Elcheroth, G., & Albzour, M. (2024). How does the geography of surveillance affect collective action? *Political Psychology, 45*(2), 319–340.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to com- puter abuse. *Journal of Information System Security, 7*(1), 24–47.

Poster, M. (1995). *The Second Media Age.* Polity Press ; B. Blackwell.

Poster, Mark. (1990). *The Mode of Information: Poststructuralism and Social Context* (1st ed.). University of Chicago Press.

Potts, J., Dopfer, K., & Tulloh, B. (2025). Explaining institutional technology. *European Economic Review, 173*, 104968.

Power, D. J. (2016). "Big Brother" can watch us. *Journal of Decision Systems, 25*(sup1), 578–588. https://doi.org/10.1080/12460125.2016.1187420

Raveendhran, R., & Fast, N. J. (2021). Humans judge, algorithms nudge: The psychology of behavior tracking acceptance. *Organizational Behavior and Human Decision Processes, 164*, 11–26.

Rosenberg, B. D., & Siegel, J. T. (2018). A 50-year review of psychological reactance theory: Do not read this article. *Motivation Science, 4*(4), 281.

Royle, O. R. (2023, February 27). *Amazon driver breaks down the A.I. system watching workers for safety violations like drinking coffee while driving and counting the times they buckle their seatbelt.* Fortune. https://fortune.com/2023/02/27/amazon-delivery-driver-breaks-down-ai-surveillance-in-vans/

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *Telematics and Informatics, 29*(2), 233–244.

Schoenherr, J. R. (2020). Understanding surveillance societies: Social cognition and the adoption of surveillance technologies. *2020 IEEE International Symposium on Technology and Society* (ISTAS), 346–357.

Seele, P. (2016). Envisioning the digital sustainability panopticon: a thought experiment of how big data may help advancing sustainability in the digital age. *Sustainability Science, 11*, 845–854.

Sum, A., Tobar, P., McLaughlin, J., & Palma, S. (2008). The great divergence: real-wage growth of all workers versus finance workers. *Challenge, 51*(3), 57–79.

Tandung, J. C. (2016). The link between HR attributions and employees' turnover intentions. *Gadjah Mada International Journal of Business, 18*(1), 55–69. https://www.antaranews.com/berita/4019463/bi-nominal-transaksi-perbankan-digital-capai-rp510303-triliun

Taylor, C., & Dobbins, T. (2021). Social media: A (new) contested terrain between sousveillance and surveillance in the digital workplace. *New Technology, Work and Employment, 36*(3), 263–284.

Thatcher, J. B., Liu, Y., Stepina, L. P., Goodman, J. M., & Treadway, D. C. (2006). IT Worker Turnover: An Empirical Examination of Intrinsic Motivation. *Data Base for Advances in Information Systems, 37*(2–3), 133–146.

Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems, 16*(2), 214–232. https://doi.org/10.1016/J.JSIS.2007.05.006

Tomczak, D. L., Lanzo, L. A., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons, 61*(2), 251–259.

Toskin, K., & McCarthy, R. V. (2019). Information Technology Work Value Differences. *Journal of Computer Information Systems,* 1–9.

Vintr, Z., Vintr, M., & Malach, J. (2012). Evaluation of physical protection system effectiveness. *2012 IEEE International Carnahan Conference on Security Technology*(ICCST), 15–21.

Vorvoreanu, M., & Botan, C. H. (2000). Examining Electronic Surveillance In The Workplace : A Review Of Theoretical Perspectives And Research Findings. In *the Conference of the International Communication Association,* 1–29.

WorkTime. (2019). *Is It Legal and Ethical To Use Employee Computer Monitoring Software?* WORKTIME.

Young, D., Carpenter, D., & McLeod, A. (2016). Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication. *AIS Transactions on Replication Research, 2*(8), 1–17.

Zhang, X., Ryan, S. D., Prybutok, V. R., & Kappelman, L. (2012). Perceived obsolescence, organizational embeddedness, and turnover of it workers: an empirical study. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 43*(4), 12–32.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power.* Basic Books, Inc.