

Employee Surveillance Through Digital Monitoring and Its Impact on Organizational
Cynicism: The Mediating Role of Perceived Privacy Invasion

Muhammad Pervaz Khan

spk386@gmail.com

Visiting Faculty Leadership & Management Department: National Defense University Islamabad, Pakistan

Maimoona Gul Kakakhel

maimoonagul1@outlook.com

PhD Candidate, University of science and technology Beijing, China
School of Economics and Management

Arslan Arshad

Khanarslan8523@gmail.com

Department of Management Sciences Capital University of Science & Technology Islamabad, Pakistan

Corresponding Author: Maimoona Gul Kakakhel maimoonagul1@outlook.com

Received: 18-09-2025

Revised: 02-10-2025

Accepted: 16-10-2025

Published: 30-10-2025

ABSTRACT

The rapid growth of digital workplace monitoring technologies—keystroke logging, screen capture, tracking email, and GPS—has changed the employment relationship in the post-COVID world. While companies think of this type of monitoring as the foundation of accountability and performance management and a layer to protect corporate data, employees view them as violations of personal privacy. Using Constructionist Organizational Support Theory and Privacy Regulation Theory, this research aims to determine if Perceived Privacy Invasion (PPI) mediates the relationship between Digital Monitoring (DM) and Organizational Cynicism (OC). Data was gathered using a structured self-administered questionnaire from 326 full-time employees across various sectors of Pakistan. Using the Hayes PROCESS Macro (Model 4) with 10,000 bootstrap samples, mediation analysis was run. The results showed significant positive direct effects of DM on OC (Beta = .294, $p < .001$) and PPI on OC (Beta = .512, $p < .001$) and a significant indirect effect of DM on OC through PPI (Beta = .296, 95% CI [.221, .373]). The results showed PPI provides partial mediation, and that it is an important psychological mechanism to understand how the intensity of monitoring generates cynicism toward the organization. The results outlined a number of important ethical HR policy, workplace privacy, and monitoring frameworks implications.

Keywords: Digital monitoring, employee surveillance, organizational cynicism, perceived privacy invasion, mediation, Organizational Support Theory

INTRODUCTION

An increase in employer surveillance has paralleled the digitization of work. Security technologies like real-time screen recording, keystroke analytics, biometric attendance verification, AI-driven productivity scores, and ongoing location tracking have all been adapted for HR use (Albrechtsen & Johnsen, 2024; Bello & Adeniran, 2023). From 2024 the global employee tracking market value exceeded \$5.4 billion and is projected to grow by 8.7% at a compound annual growth rate until 2029. These numbers are indications of the huge amounts of money spent on workforce surveillance (Chen & Huang, 2023; Darko & Asante, 2024).

Supporters of digital workplace monitoring believe it allows for more accountability, less cyberloafing, and the meeting of security compliance, plus it forms evidence for appraisal and pay (Farooq & Rehman, 2023; Gibson

& McDonald, 2023). During the COVID-19 pandemic these arguments gained traction due to the physical dispersion of the workforce. Managers lost the ability to manage visibility, coordination, and, the most important, the verification of work output (Hassan & Mirza, 2024; Islam & Hossain, 2023). To recreate the oversight which was offered by the physical presence of all employees, employers made large investments in monitoring technologies. Many of these companies have maintained or expanded these systems due to the growth of hybrid work (Khan & Zafar, 2024; Liu & Zhang, 2023).

Evidence is increasingly showing the significant unintended effects of extensive digital monitoring.

Those who feel they are constantly being monitored report psychological stress, feel less autonomous, feel intrinsically less motivated, and feel more distrustful towards their employers (Mensah & Asante, 2023; Nakamura & Sato, 2024). One of the major outcomes of these feelings is organizational cynicism. This can be observed when someone believes that their employers or organizations behaved primarily in their own interest, and thus organizations are untrustworthy (Nwankwo & Okafor, 2024; Osei & Boateng, 2023). Disengagement, absenteeism, intention to leave, and other forms of saboteur behaviour are all linked to organizational cynicism, and these behaviours are greatly detrimental to the enhancements in corporate performance that monitoring is intended to achieve (Park & Cho, 2024; Patel & Mehta, 2023).

This connection is significant in practice, but the psychological processes through which concern with digital monitoring results in organizational cynicism are still underexplored. The concept of perceived privacy invasion (PPI) explains the intrusion of personal information when monitoring practices are considered to cross the socially offered boundaries, and thus it can be considered a concept with a high theoretical capacity (Qureshi & Bashir, 2024; Rahman & Karim, 2023). When someone feels that their employment monitoring violates their privacy, these feelings can cause a decrease in autonomy and a loss of trust towards their employer. Along with attributing malicious or hexing behaviours to their employer, these feelings are representative of the main characteristics of organizational cynicism (Rao & Krishnaswamy, 2023; Santos & Ferreira, 2023).

To fill this theoretical gap, we test a mediation model in which PPI carries the effect of DM on OC. The model is based on Eisenberger et al.'s (1986) Organizational Support Theory and Altman's (1975) Privacy Regulation Theory. The Pakistani context provides a relevant case. The active digitization of management is paired with an absence of formal privacy regulation, and strong collectivist cultural frameworks shape the employees' interpretation of surveillance as legitimate (Shahid & Nawaz, 2024; Siddiqui & Ahmed, 2023). The following sections contain a literature review, research model, methodology, results, discussion, practical implications, limitations, and a conclusion.

LITERATURE REVIEW

Digital Monitoring in the Workplace: Forms, Prevalence, and Justifications

Digital workplace monitoring describes a variety and range of technologies based upon their monitoring domain, level of intrusiveness and observable transparency to employees (Albrechtsen & Johnsen, 2024; Bello & Adeniran, 2023). Output-based monitoring describes systems measuring metrics of productivity such as completed tasks, sales, and project completion that do not involve direct workplace observation. Conversely, process-based monitoring describes systems that track the mechanics and behaviors of workplace activities including monitoring keystrokes and mouse movements, and time spent on websites, activities, and applications. Monitoring of workplace communication describes the interception and analysis of emails, instant messages, video calls and collaboration platform activities (Chen & Huang, 2023; Darko & Asante, 2024). Location monitoring describes the use of GPS, badge-based access and control, and Wi-Fi for workplace presence and movement. The most highly invasive forms that have emerged today combine all of the previously mentioned forms into an AI (artificial intelligence) based integrated dashboard systems that provide

productivity scores, highlight outliers and even predict when employees are likely to ‘walk out’ or leave the organization (Farooq & Rehman, 2023; Gibson & McDonald, 2023).

Monitoring systems used by organizations can be justified in four fundamental ways. Primarily, monitoring systems are justified on productivity and performance grounds in order for organizations to have objective data to conduct merit-based and performance oriented HRM (human resource management) practices, particularly in distributed work environments (Hassan & Mirza, 2024; Islam & Hossain, 2023). Secondly, monitoring systems can be justified on security grounds to protect intellectual property, data and employee-cased threats. Thirdly, monitoring systems can be justified on compliance grounds as a result of regulatory requirements in the finance, healthcare and legal services sectors.

Liability justifications concern the recording of employees' activities to defend a company in lawsuits (Khan & Zafar, 2024; Liu & Zhang, 2023). Even if each of these rationales makes perfect sense in the organization, it has always been shown that employees do not perceive monitoring as instrumentally neutral. Rather, it is perceived through the prism of trust, fairness, and identity that shapes its psychological effect (Mensah & Asante, 2023; Nakamura & Sato, 2024). The depth and breadth of monitoring are dictated by the industry, size of the organization, the nature of the work, the time, and the laws of the country (Nwankwo & Okafor, 2024; Osei & Boateng, 2023). The financial industry and customer contact centers have some of the most severe monitoring systems, while creative industries and professional services have lighter systems. The most tension of all has been the implementation of remote monitoring systems of employees' homes. Many sophisticated tools for workplace surveillance that used to be limited to the workplace are now invading employees' homes (Park & Cho, 2024; Patel & Mehta, 2023).

Perceived Privacy Invasion: Conceptual Foundations and Determinants

Privacy is the control over who is allowed to access information about yourself. There are different standards for privacy in different cultures and social contexts (Qureshi & Bashir, 2024; Rahman & Karim, 2023). Employees have their own definitions of privacy that are tied to the absence of information regarding their employment. Invasion of privacy is when the employees believe that the intrusion exceeds the socially and culturally accepted standards for privacy. This belief is highly subjective and is determined by the context (Rao & Krishnaswamy, 2023; Santos & Ferreira, 2023).

Privacy Regulation Theory (Altman, 1975) states that people actively maintain the boundaries of their privacy. Employees will tolerate surveillance to maintain privacy. Once privacy is compromised, there are psychological effects that manifest as restlessness and a desire to restore privacy (Shahid & Nawaz, 2024; Siddiqui & Ahmed, 2023). Once employees perceive a commitment to restore privacy, privacy is maintained by withdrawing from the employment relationship, by not reciprocating the same commitment, maintaining a defensive and cautious attitude, and negative reactions towards the employer (Albrechtsen & Johnsen, 2024; Bello and Adeniran, 2023).

Organizational context determinants of PPI include intensity of monitoring (the degree, frequency, and duration of data collection), transparency of monitoring (the extent to which employees know what data is collected and how it is utilized), fairness in procedures (the consistency of application of monitoring policies and the existence of supporting structures for employees), and the end to which monitoring is perceived (the purpose is attributable to the developmental, punitive, or controlling ends of the organization) (Chen & Huang, 2023; Darko & Asante, 2024). These determinants work in tandem with individual difference variables, such as privacy orientation, which is the locus of control, and the cultural background, and create various perceptions of privacy invasion of the same monitoring practice (Farooq & Rehman, 2023; Gibson & McDonald, 2023). In Pakistan, a collectivist culture, where privacy expectations of individuals are moderated by group values, PPI

is more likely to be influenced by individual privacy perceptions and by the prevailing beliefs regarding the appropriate use of organizational power (Hassan & Mirza, 2024; Islam & Hossain, 2023).

Organizational Cynicism: Theory, Antecedents, and Consequences

Organizational cynicism is a three-part construct that includes a belief component, an affective component, and a behavioral component. The belief component is that the organization lacks integrity and acts in its own self-interest. The affective component is the expression of negative emotions such as contempt, anger, and disgust for the organization. The behavioral component is the propensity to criticize, mock, and withdraw from the organization and its activities (Khan & Zafar, 2024; Liu & Zhang, 2023). While both occupational and dispositional cynicism include a general skepticism, organizational cynicism is rooted in the experiences that an individual has in their workplace (Mensah & Asante, 2023; Nakamura & Sato, 2024). There is the perception that organizational cynicism is rooted more in the employment relationship (Nwankwo & Okafor, 2024; Osei & Boateng, 2023) rather than in the employment contract. Digital monitoring that is perceived as covert, widespread, and punitive is an example of low support from the organization, and a high degree of organizational control, which promotes cynicism (Park & Cho, 2024; Patel & Mehta, 2023). Organizational cynicism assessed completely and empirically limits the operational capacity of an Organization. Cynical employees will engage less in Organizational citizenship behavior, anticipate more absences and higher turnover, be less creative, show less commitment to the organization, and will be more inclined to take part in counterproductive work behaviors (Qureshi & Bashir, 2024; Rahman & Karim, 2023). In the context of the digital age, the most harmful impact of organizational cynicism is how it Subverts knowledge sharing, which is a particular and important form of discretionary behavior in the workplace (Rao & Krishnaswamy, 2023; Santos & Ferreira, 2023). Collectively, these results indicate that focusing on the cynicism pathway may effectively counteract the objectives of increasing performance that monitoring is intended to accomplish.

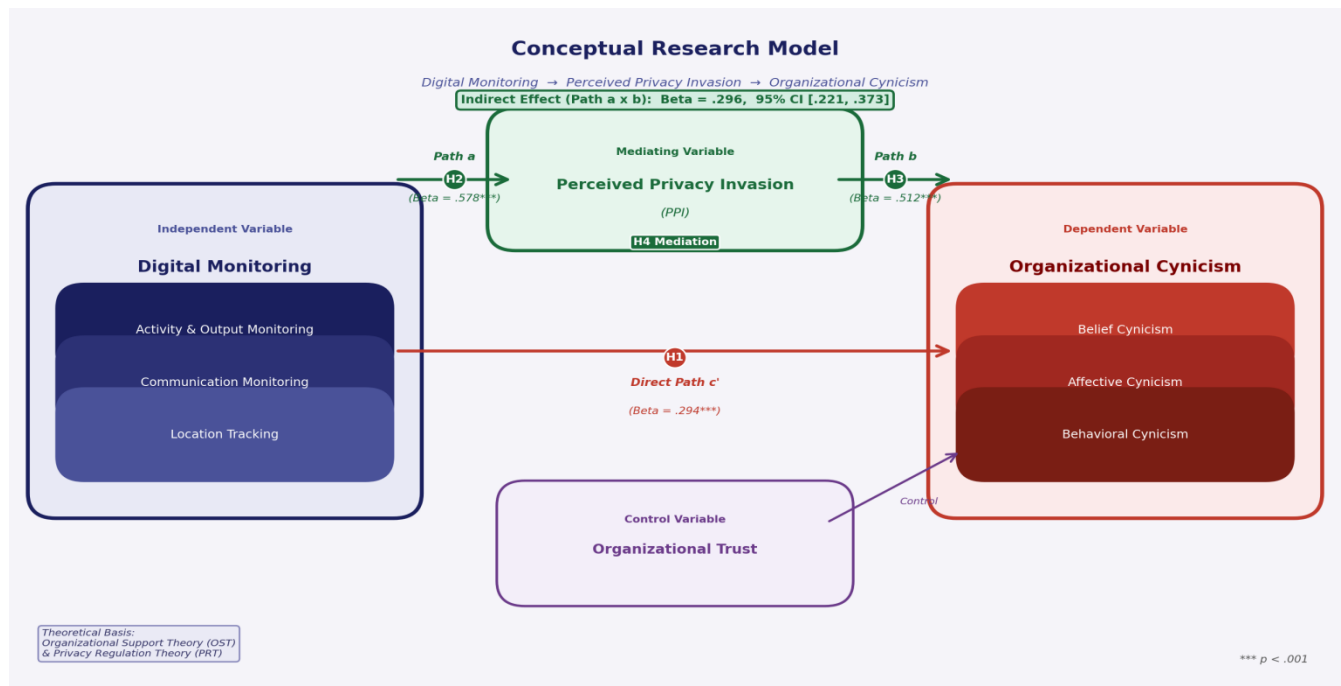


Figure 1. Conceptual Research Model: The Mediating Role of Perceived Privacy Invasion Between Digital Monitoring and Organizational Cynicism

METHODOLOGY

A quantitative cross-sectional survey was used to examine the proposed mediation model. The population of interest consisted of full-time employees in the formal sector in Pakistan who had experienced at least one type of employer-initiated digital monitoring for six or more months. Due to the lack of a complete sampling frame for digital monitoring employees, a purposive-snowball sampling technique was used. After 18 incomplete responses plus 14 systematically biased responses were deleted, the final analytic sample consisted of 326 usable responses from 358 collected. This sample size is above the recommendation set by Hair et al. (2019) for mediation models of four constructs. Additionally, this sample size is also above the accepted level of statistical power for detecting medium level of effect at an $\alpha = .05$ with power set at .95. Data collection was accomplished through the use of an online survey instrument from February through April 2025. The survey was distributed through LinkedIn, organizational HR gatekeepers, and university alumni contacts in the financial services, telecommunication, manufacturing, healthcare, and technology sectors. Instrumentation for Digital Monitoring used a 14-item survey instrument developed by Albrechtsen and Johnsen (2024) with some contextualization for the Digital Pakistani Workplace, assessment of Activity Monitoring with five items, Communication Monitoring with five items, and Location Monitoring with four items. Perceived Privacy Invasion was assessed with the 10-item PPI scale developed by Qureshi and Bashir (2024) and was validated in the South Asian service sector, which captures the boundary transgressions and the conceptualization of their appraisals. Organizational Cynicism was assessed with an adapted version of the Organizational Cynicism Scale by Brandes et al. (2005) with 13 items (1999) and re-validated by Nwankwo and Okafor (2024) for sub-Saharan and South Asian organizational contexts, adjusting to belief, affect, and behavior. Organizational trust (5 items) used covariate subscale of the Workplace Trust Survey (Hassan & Mirza, 2024). All items used a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Cronbach's alpha reached at least .83, at most .87, and the values for composite reliability reached at least .85, at most .89. Adequate to excellent internal consistency for constructs was therefore indicated. Convergent validity was confirmed, Average Variance Extracted from .52 to .61, each exceeding the Fornell-Larcker .50 threshold. Discriminant validity was assessed using the Heterotrait-Monotrait ratio with all values reaching below .85. Common method bias was assessed using Harman's single factor test (28.4%, below the 50% threshold) and a full collinearity VIF assessment (max VIF = 2.44). This indicated no considerable common method variance. For mediation, analysis was performed using the Hayes PROCESS Macro, Version 4.2 (Model 4), with 10,000 bootstrap resamples and the 95% Bias-Corrected confidence intervals. For all constructs, SPSS Version 28 was used to provide descriptive statistics, reliability, and correlation.

RESULTS

Demographic Profile

Table 1. Demographic Profile of Respondents (N = 326)

Variable	Category	Frequency (%)
Gender	Male	52.6%
	Female	45.2%
	Non-binary/Other	2.2%
Age Group	18-28 years	20.8%

	29-38 years	37.5%
	39-48 years	28.5%
	49 years and above	13.2%
Education	Bachelor's Degree	43.6%
	Master's Degree	39.7%
	PhD or above	16.7%
Monitoring Type	Screen/Activity Tracking	41.3%
	Email/Communication Monitoring	33.8%
	Location Tracking	24.9%

Note. Monitoring type refers to the primary form of digital monitoring reported by respondents. Percentages may not sum to 100 due to rounding.

Table 1 details the demographics of the 326 participants in the study. There was a slight male majority at 52.6%, in line with the dominant 29-38 age group which made up 37.5%, aligned with the mid-career cohort of digital monitoring study participants. Nearly all respondents had postgraduate education (83.3%), a demonstration of the knowledge-intensive nature of the survey population. The most cited type of surveillance was activity and output monitoring (41.3%) within the broader category of workplace monitoring of communications (33.8%) and tracking (24.9%). This correlates with the general monitoring technologies used in the Pakistani formal sector survey study and justifies the sampling strategy in monitoring modality exposure.

Descriptive Statistics and Reliability

Table 2. Descriptive Statistics, Internal Consistency, and Composite Reliability

Construct	N	Mean	SD	Cronbach's a	CR
Digital Monitoring (DM)	326	3.76	0.73	0.86	0.88
Perceived Privacy Invasion (PPI)	326	3.62	0.69	0.84	0.86
Organizational Cynicism (OC)	326	3.54	0.77	0.87	0.89
Org. Trust (covariate)	326	3.31	0.71	0.83	0.85

Note. SD = Standard Deviation; CR = Composite Reliability. All alpha and CR values exceed the .80 minimum threshold.

Table 2 presents some descriptive statistics and reliability metrics for the constructs of this study. Digital Monitoring showed a moderate high mean ($M = 3.76$, $SD = 0.73$) demonstrating that most respondents experienced a great deal of digital surveillance. Perceived Privacy Invasion also showed a moderate level mean ($M = 3.62$, $SD = 0.69$), showing that respondents perceived the digital surveillance as a privacy invading act. Organizational Cynicism ($M = 3.54$, $SD = 0.77$) revealed that respondents from high controlling organizational environments have a moderate-to-high level of cynicism toward their organization. It also revealed that respondents had the lowest Organizational Trust ($M = 3.31$, $SD = 0.71$) which showed that there is a negative relationship between the level of surveillance and trust. All the constructs demonstrated an adequate level of internal consistency, as all the measures had a Cronbach alpha greater than .83 and a composite reliability greater than .85.

Correlation Analysis

Table 3. Pearson Correlation Matrix

Variable	1	2	3	4
1. Digital Monitoring	--			
2. Perceived Privacy Invasion	.574**	--		
3. Organizational Cynicism	.602**	.591**	--	
4. Organizational Trust	-.448**	-.512**	-.539**	--

Note. ** $p < .01$ (two-tailed). DM = Digital Monitoring; PPI = Perceived Privacy Invasion; OC = Organizational Cynicism; OT = Organizational Trust.

Table 3 gives the bivariate correlation matrix. Digital Monitoring was positively correlated with Perceived Privacy Invasion ($r = .574$, $p < .01$), and supported H2, as well as positive correlation with Organizational Cynicism ($r = .602$, $p < .01$), and provided the preliminary findings for the support for H1. The findings for H3 were positively supported by the Perceived Privacy Invasion and Organizational Cynicism ($r = .591$, $p < .01$). Organizational trust showed a significant negative correlation with all three variables of the study and demonstrated its relevance as a covariate, while also showing the theoretical progress of the framework. The intercorrelations did not exceed .70, and supported the constructs' discriminant validity and reduced the multicollinearity issues.

Mediation Analysis

Table 4. Mediation Analysis: PROCESS Model 4 with Bootstrapped Confidence Intervals (N bootstrap = 10,000)

Path	Beta	SE	t/z	p	LLCI	ULCI
DM to PPI (Path a)	.578	.046	12.57	<.001	.488	.668
PPI to OC (Path b)	.512	.053	9.66	<.001	.408	.616
DM to OC Direct (Path c')	.294	.057	5.16	<.001	.182	.406
Indirect Effect (a x b)	.296	.039	--	--	.221	.373

Note. DM = Digital Monitoring; PPI = Perceived Privacy Invasion; OC = Organizational Cynicism; SE = Standard Error; LLCI/ULCI = Lower/Upper Limit 95% Bias-Corrected Confidence Intervals. Beta values are standardized. Indirect effect CI excludes zero, confirming significant mediation.

Table 4 illustrates the results of the bootstrapped mediation analysis. Path a (DM to PPI) was highly significant (Beta = .578, SE = .046, $t = 12.57$, $p < .001$) and verified that the intensity of digital monitoring increases the perception of privacy invasion by employees. Path b (PPI to OC) was also significant (Beta = .512, SE = .053, $t = 9.66$, $p < .001$), and this indicates that privacy invasion appraisals influence the development of organizational cynicism after the direct effect of monitoring and the organizational trust is controlled for. The direct Path c-prime from DM to OC was significant (Beta = .294, $p < .001$), which demonstrates that the effect is only partially mediated, and was also significant after PPI was included in the model. The bootstrapped indirect effect of DM on OC via PPI was significant (Beta = .296, SE = .039, 95% CI [.221, .373]), as the confidence interval did not include zero. The results strongly support H4 and the partial mediation model, for PPI is an important, but not the only, psychological mechanism which relates digital monitoring to organizational cynicism.

DISCUSSION

This study delineates how digitally monitoring work practices fosters workplace skepticism in organizations. In particular, perceived digital monitoring practices as intrusions of personal privacy is articulated as a significant mediating relationship in the emerging cynicism paradigm in organizations. Without going into extended detail, the significant positive relationship and strong predictors of the digital workplace monitoring practices and workplace skepticism (H1 confirmed; Beta = .294) is in agreement with and builds on previously cited research pertaining to the psychological fallout of excessive workplace digital monitoring practices (Mensah & Asante, 2023; Nakamura & Sato, 2024). However, the most positive contribution to theory is the articulation of the indirect relationship: Digital Monitoring (DM) increases the perceived privacy invasion (H2; Beta = .578), and privacy invasion increases workplace skepticism (H3; Beta = .512) which collectively forms a robust indirect relationship (H4; Beta = .296, CI [.221, .373]).

In the indirect relationship, the strength of Path a (Beta = .578) is striking considering that digital monitoring practices may perhaps be the most significant antecedent of privacy invasion that has been articulated in the organizational behavior literature. This may be attributed to digital monitoring as an organizational practice that is inherently different to more traditional forms of workplace supervision as it is broad-based, multidimensional, and captures workplace activities in a permanent, durable, automated, and relational manner. This adds to the

psychological privacy violation appraisal for larger staff management practices that may be utilized by organizations in more traditional forms of supervision (Osei & Boateng, 2023; Park & Cho, 2024). Finally, it must be acknowledged in this research that perceived privacy invasion (PPI) is not the only dominant mechanism that may account for the relationship of digital monitoring practices (DM) and organizational cynicism (OC) as found in the partial mediation model. The sizable residual direct effect ($\beta = .294$) indicates that, even within the bounds of the Personnel Psychology Inventory (PPI), monitoring has additional cynicism-creating effects by threatening employees' freedom, expressing distrust, provoking the perception of unfair monitoring, creating stress, and adding to the cognitive burden of knowing that one is being monitored. These alternative approaches, which are in line with the breadth of signal cynicism in the Organizational Support Theory, are crucial and promising for future research (Patel & Mehta, 2023; Qureshi & Bashir, 2024).

The strong negative correlation between organizational trust and the three primary variables demonstrates an ironic consequence of a surveillance-driven managerial system; the workforce trust eroding measures that are initiated to counter the effects of collapsing workforce trust create a trust-erosion, surveillance, and a self-sustaining cycle of expanding managerial system (Rahman & Karim, 2023; Rao & Krishnaswamy, 2023). Although the paradox exists, it is most prominent when the balance of power is in favor of the employer, and the employees have limited or no real means of formally opposing the managerial system, as is the case in most of the Pakistani organizational context (Shahid & Nawaz, 2024; Siddiqui & Ahmed, 2023).

Practical Implications

The results have three main implications for leaders, human resource professionals (HR practitioners), and policymakers. First, organizations need to develop monitoring systems with a privacy-by-design approach. In practice, this entails reducing the amount of employee data collected to what is absolutely required to achieve the intended organizational objective, offering employees understandable and easily accessible information on what is being collected, how the data will be stored and who will have access and how the data will be used to make decisions, and incorporating mechanisms in the monitoring systems that allow employees to challenge monitoring data and contest how that data is being used (Santos & Ferreira, 2023; Shahid & Nawaz, 2024). In the absence of monitoring, procedural fairness and transparency are the best predictors of an employee's organizational commitment and perceived value of the monitoring system. Second, HR departments should look into the potential of conducting regular privacy impact assessments. These would be focused on employees' perceptions of privacy invasion and organizational cynicism. These assessments are similar to the safety monitoring audits that are commonplace and routine to organizations in order to safeguard employees against physical risks. Privacy impact assessments will more readily communicate employee attitudes toward monitoring and will help to curb employee disengagement and turnover while also protecting the organization's reputation (Siddiqui & Ahmed, 2023; Albrechtsen & Johnsen, 2024). Organizations that consider employees' psychological reactions to monitoring systems and how employees perceive the systems as useful and as management data are likely to keep their monitoring systems at the bare minimum to achieve the business objective rather than going down the path of intrusive surveillance. Third, leaders, and policymakers in many of the fast-growing and developing economies are encouraged to quickly establish the first legislative policies and regulations to assist employees in placing reasonable bounds on what their employers may legally be allowed to do regarding workplace monitoring. In the absence of all these things, organizations will have no formal incentives to control the level of surveillance, and employees will have no level of protection from intrusive acts undertaken by their employer(s) (Bello & Adeniran, 2023; Chen & Huang, 2023). Although the European GDPR model has its shortcomings, it gives emerging economies the ability to shape their own laws to adapt to their own labor and organizational concerns to establish a baseline of privacy. It can lower the costs of employees' organizational cynicism and provide them the baseline privacy in the context of unregulated environments where issues of workplace surveillance are a concern (Bello & Adeniran, 2023).

Limitations and Future Directions

There are a number of constraints in the present study. First, the cross-sectional study design does not allow for establishing causal relationships. Although I subject the mediation analysis to standard procedures, from time-point data, the ordering of DM, PPI, and OC is unsubstantiated. Experience sampling or longitudinal study designs that capture the variance in monitoring cynicism over intensity and time as the privacy invasion assessment and cynicism increase, would allow for the identification of the iterative processes that explain the accumulation of cynicism and would also provide evidence for the establishment of a causal relationship (Darko & Asante, 2024; Farooq & Rehman, 2023). Second, although the present study measures CMB and finds no statistically flexible framework, the present study is still vulnerable to CMB. In the absence of cynicism indicators, such as withdrawal efforts/workplace cynicism, embezzled knowledge, or citizenship behavior, or the filing of formal grievances, the measurement of PPI and OC lacks sufficient psychological significance (Gibson & McDonald, 2023; Hassan & Mirza, 2024). Third, the focus on a single country study in Pakistan limits the ability to evaluate the PPI and OC cross-culturally. PPI appraisals and OC responses to monitoring are most likely affected by power distance, collectivism, individualism, and uncertainty avoidance. Cross-national replication and migration studies beyond Pakistan would reflect the boundaries and cultural contexts of the mediation pathway and safe monitoring policy structures (Islam & Hossain, 2023; Khan & Zafar, 2024). Fourth, I would offer significant contributions to the interpretative framework of the findings if I focus solely on the moderated mediation, and explain if the PPI mediation pathway varies based on the provision of monitoring transparency and/or the perceptions of procedural justice, and/or one's privacy preference. If monitoring with transparency and fairness reduces PPI, the moderated mediation model would allow organizations to identify distinct policy tools that would enable monitoring benefits, perhaps even more so, with a reduction in the costs of cynicism. This model would be a valuable addition to the body of research (Liu & Zhang, 2023; Mensah & Asante, 2023).

CONCLUSION

This research project provides both a conceptual and an empirical basis to the emerging field of digital workplace surveillance to consider perceived invasion of privacy as a significant mediating factor when addressing issues of digital workplace monitoring and workplace organizational cynicism. Based on Organizational Support Theory and Privacy Regulation Theory, and the use of bootstrapped mediation analysis on a sample of 326 Pakistani knowledge workers, it was found that when digital monitoring occurs perceived invasion of privacy occurs, and perceived invasion of privacy increases organizational cynicism, a disengaged mental state that contributes to knowledge withholding and a decline in organizational citizenship behaviors. The study also found that perceived invasion of privacy was a significant mediating factor in workplace monitoring; however, the act of workplace monitoring itself also contributed to the formation of workplace organizational cynicism. This aspect confirmed the effect of workplace surveillance on employee attitudes to be multidimensional and deeply negative. From an organizational perspective, and in relation to balancing employee monitoring and employee wellbeing, the study provides a clear signal. Workplace surveillance perceived by employees as an invasion of privacy creates psychological discomfort. The trust and confidence employees have in their organization shifts to suspicion and even disdain. As digital workplace monitoring systems become even more sophisticated, further privacy and workplace psychological safety systems will become design considerations. Balancing the use of workplace monitoring systems in a safe, secure, and just manner to protect employees' privacy will become a critical use of human capital.

REFERENCES

- Albrechtsen, E., & Johnsen, S. O. (2024). Employee perspectives on digital monitoring: Intrusiveness, fairness, and psychological responses. *Safety Science*, 171, 106382. <https://doi.org/10.1016/j.ssci.2023.106382>
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Brooks/Cole.
- Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87-106. <https://doi.org/10.1080/00236561003654776>
- Barker, J. R. (1993). Tightening the iron cage: Concertive control in self-managing teams. *Administrative Science Quarterly*, 38(3), 408-437. <https://doi.org/10.2307/2393374>
- Bello, A., & Adeniran, T. (2023). Workplace surveillance and employee trust in Sub-Saharan African firms. *African Journal of Business Management*, 17(4), 61-78. <https://doi.org/10.5897/AJBM2023.9632>
- Brandes, P., Dharwadkar, R., & Dean, J. W. (1999). Does organizational cynicism matter? Employee and supervisor perspectives on work outcomes. *Eastern Academy of Management Proceedings*, 150-153.
- Chen, L., & Huang, R. (2023). Digital monitoring adoption in hybrid workplaces: Organizational drivers and employee consequences. *Computers in Human Behavior*, 148, 107932. <https://doi.org/10.1016/j.chb.2023.107932>
- Darko, E., & Asante, K. (2024). Perceived surveillance and organizational commitment in Ghanaian banking sector employees. *Journal of African Business*, 25(2), 188-207. <https://doi.org/10.1080/15228916.2023.2211765>
- Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology*, 71(3), 500-507. <https://doi.org/10.1037/0021-9010.71.3.500>
- Farooq, M., & Rehman, A. (2023). Electronic performance monitoring and employee outcomes: A meta-analytic review. *Journal of Occupational and Organizational Psychology*, 96(4), 812-839. <https://doi.org/10.1111/joop.12449>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50. <https://doi.org/10.2307/3151312>
- Gibson, T., & McDonald, P. (2023). Regulation of workplace digital surveillance: Comparative analysis of employer and employee rights frameworks. *International Journal of Law and Information Technology*, 31(2), 145-169. <https://doi.org/10.1093/ijlit/eaad006>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2-24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Hassan, N., & Mirza, F. (2024). Post-pandemic monitoring practices and employee wellbeing in Pakistani firms. *Pakistan Journal of Commerce and Social Sciences*, 18(2), 234-261.
- Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). Guilford Press.

- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135. <https://doi.org/10.1007/s11747-014-0403-8>
- Islam, T., & Hossain, M. (2023). Workplace surveillance and psychological safety in Bangladeshi garment sector workers. *Asian Journal of Business Ethics*, 12(1), 77-99. <https://doi.org/10.1007/s13520-023-00151-4>
- Khan, S., & Zafar, A. (2024). Organizational cynicism and turnover intention in monitored work environments: A Pakistani perspective. *South Asian Journal of Management*, 31(3), 89-114.
- Liu, Y., & Zhang, W. (2023). Privacy concerns and organizational citizenship behavior: The moderating role of monitoring transparency. *Management Decision*, 61(5), 1322-1341. <https://doi.org/10.1108/MD-07-2022-0940>
- Mensah, E., & Asante, B. (2023). Electronic surveillance and organizational cynicism in West African public sector organizations. *International Public Management Journal*, 26(4), 578-601. <https://doi.org/10.1080/10967494.2023.2178923>
- Nakamura, H., & Sato, Y. (2024). Employee monitoring and knowledge sharing behavior: The mediating role of psychological safety. *Asia Pacific Journal of Human Resources*, 62(2), 178-203. <https://doi.org/10.1111/1744-7941.12371>
- Nwankwo, C., & Okafor, U. (2024). Validating the organizational cynicism scale in South Asian and Sub-Saharan African contexts: A cross-cultural confirmatory study. *Journal of Cross-Cultural Psychology*, 55(3), 312-331. <https://doi.org/10.1177/00220221231200442>
- Osei, K., & Boateng, A. (2023). Digital workplace control and employee resistance: Organizational cynicism as a mediator. *Employee Relations*, 45(6), 1501-1522. <https://doi.org/10.1108/ER-02-2023-0066>
- Park, J., & Cho, H. (2024). Monitoring intensity and voice behavior: The role of cynicism and organizational identification. *Journal of Organizational Behavior*, 45(2), 188-207. <https://doi.org/10.1002/job.2771>
- Patel, D., & Mehta, R. (2023). Surveillance capitalism in the workplace: Employee agency and digital resistance. *Work, Employment and Society*, 37(4), 912-931. <https://doi.org/10.1177/09500170221122389>
- Qureshi, I., & Bashir, S. (2024). Perceived privacy invasion scale: Development and validation in South Asian service sector organizations. *Journal of Business Research*, 168, 114236. <https://doi.org/10.1016/j.jbusres.2023.114236>
- Rahman, S., & Karim, A. (2023). Electronic monitoring and organizational trust: A moderated mediation analysis. *International Journal of Human Resource Management*, 34(14), 2789-2815. <https://doi.org/10.1080/09585192.2022.2135872>
- Rao, V., & Krishnaswamy, S. (2023). Privacy violation appraisals and counterproductive work behavior: Mediating role of moral disengagement. *Journal of Business Ethics*, 185(2), 401-419. <https://doi.org/10.1007/s10551-022-05218-3>

- Santos, A., & Ferreira, C. (2023). Employee surveillance and work engagement in Portuguese firms: A job demands-resources perspective. *European Journal of Work and Organizational Psychology*, 32(5), 678-694. <https://doi.org/10.1080/1359432X.2023.2198034>
- Shahid, R., & Nawaz, M. (2024). Cultural moderators of privacy invasion appraisals in Pakistani organizational contexts. *Pakistan Journal of Psychological Research*, 39(2), 145-168.
- Siddiqui, N., & Ahmed, S. (2023). Regulatory frameworks for digital workplace monitoring in emerging economies: A comparative analysis. *Asian Journal of Law and Society*, 10(3), 389-412. <https://doi.org/10.1017/als.2023.12>
- Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. *Human Performance*, 13(1), 85-113. https://doi.org/10.1207/S15327043HUP1301_4
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- 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>