



Digital Surveillance and Employee Trust: The Mediating Role of Privacy Concerns

Furqan ul Haq Siddiqui

Director BIC, University of Balochistan, Quetta

Email: furqan.ims@um.uob.edu.pk

Abstract: Digital surveillance has become increasingly common in contemporary workplaces as organizations adopt monitoring software, productivity tracking systems, biometric technologies, location tracking, electronic communication monitoring, artificial intelligence based analytics, and other digital technologies to manage organizational activities. Although digital surveillance can support productivity, security, compliance, performance management, and organizational risk control, excessive or poorly governed monitoring may generate employee concerns regarding privacy, autonomy, fairness, and the appropriate use of personal information. These concerns may influence the level of trust employees place in their organizations. This study examines the relationship between digital surveillance and employee trust and investigates the mediating role of privacy concerns. Digital surveillance is conceptualized as the extent to which organizations electronically monitor employee activities, communications, location, productivity, system usage, and behavioral patterns. Privacy concerns represent employees' perceptions that organizational surveillance may intrude upon personal privacy, collect excessive information, use data beyond its intended purpose, or provide insufficient control over personal information. Employee trust represents employees' confidence that their organization and management will act fairly, responsibly, transparently, and in employees' interests. The study is theoretically grounded in Organizational Trust Theory, Social Exchange Theory, and Privacy Calculus Theory. A quantitative cross sectional research design is proposed using a structured questionnaire administered to employees working in organizations where digital monitoring technologies are used. A five point Likert scale can be employed to measure the three constructs. Partial Least Squares Structural Equation Modeling using Smart PLS is recommended because it can assess latent variables and mediation relationships simultaneously. The illustrative results indicate that digital surveillance has a significant positive relationship with privacy concerns, while privacy concerns have a significant negative relationship with employee trust. Digital surveillance also demonstrates a significant negative direct relationship with employee trust. Mediation analysis indicates that privacy concerns significantly mediate the relationship between digital surveillance and employee trust. The findings suggest that employees may perceive extensive digital monitoring as a threat to privacy, which can weaken their confidence in organizational management. The study contributes to workplace technology literature by explaining privacy concerns as an important mechanism through which surveillance practices can influence employee trust. Practical implications include establishing transparent surveillance policies, limiting data collection to legitimate purposes, obtaining appropriate

consent, ensuring data security, providing employees with information about monitoring practices, and developing clear mechanisms for challenging inappropriate surveillance. The study concludes that digital surveillance should be implemented responsibly because technological monitoring without adequate privacy protection may undermine employee trust and organizational relationships.

Keywords: Digital Surveillance, Employee Trust, Privacy Concerns, Workplace Monitoring, Employee Privacy, Organizational Trust, Digital Workplace, Electronic Monitoring, Employee Relations, Smart PLS

Introduction

The rapid development of digital technologies has transformed workplace management. Organizations increasingly use digital systems to monitor employee productivity, communications, attendance, location, system activity, customer interactions, and work patterns. Technologies such as employee monitoring software, biometric systems, GPS tracking, video surveillance, keystroke monitoring, email analytics, artificial intelligence, and productivity dashboards have become increasingly accessible.

Digital surveillance can provide organizations with important operational benefits. Employers may use monitoring systems to improve workplace security, protect organizational information, measure productivity, identify operational problems, ensure regulatory compliance, and coordinate distributed workforces.

However, workplace surveillance also creates important concerns regarding employee privacy. Employees may question what information is being collected, why it is being collected, who can access it, how long it will be retained, and whether it will be used for purposes beyond those originally communicated.

Privacy concerns become particularly important when monitoring technologies collect information continuously or invisibly. Employees may feel that their autonomy is reduced when they believe that every digital activity is subject to organizational observation.

Employee trust is a critical component of organizational functioning. Trust refers to employees' willingness to rely on management and organizational systems despite uncertainty and vulnerability. High levels of trust can support cooperation, communication, commitment, knowledge sharing, and organizational citizenship behaviors.

Digital surveillance may influence trust because monitoring communicates information about the relationship between employees and management. When surveillance is perceived as transparent, proportionate, and legitimate, employees may accept it as an organizational security or performance management mechanism. When surveillance is perceived as excessive or intrusive, employees may interpret it as evidence that management does not trust them.

Privacy concerns may represent the psychological mechanism connecting surveillance with employee trust. Digital surveillance can increase employees' perceptions that their personal information is being collected or used without sufficient control. These perceptions can create discomfort, uncertainty, and concerns about organizational intentions.

The relationship between surveillance and trust is therefore complex. Surveillance may provide legitimate organizational benefits while simultaneously creating perceptions of intrusion.

Privacy Calculus Theory suggests that individuals evaluate potential benefits and risks associated with information disclosure and technological systems. Employees may accept monitoring when perceived organizational benefits outweigh perceived privacy risks. Conversely, strong privacy concerns may lead to resistance or negative attitudes.

Social Exchange Theory provides another theoretical perspective. Employment relationships involve reciprocal expectations between employees and organizations. Employees who believe that their organization respects their privacy and treats them fairly may reciprocate with trust and positive attitudes. Excessive monitoring may violate these expectations and weaken the exchange relationship.

Organizational Trust Theory further emphasizes fairness, integrity, competence, benevolence, and predictability. Surveillance practices can affect perceptions of these dimensions, particularly when employees believe that monitoring lacks transparency or fairness.

The increasing adoption of remote and hybrid work has intensified the relevance of this issue. Organizations may use digital surveillance technologies to monitor employees who work outside traditional office environments. Although such systems may help managers coordinate distributed work, employees may perceive continuous monitoring as invasive.

The issue is also important because surveillance technologies increasingly use artificial intelligence and automated analytics. AI systems can potentially analyze communication patterns, productivity behavior, facial expressions, location information, and other forms of employee data. These developments raise questions concerning transparency, accountability, bias, and employee autonomy.

Despite growing interest in digital workplace technologies, the psychological mechanisms linking surveillance to employee trust require further examination. Understanding privacy concerns as a mediator can help explain why monitoring practices may produce negative employee reactions.

This study therefore examines the relationship between digital surveillance and employee trust and investigates whether privacy concerns mediate this relationship.

The research has theoretical significance because it integrates workplace surveillance, privacy, and organizational trust perspectives into a single empirical framework.

The study also has practical importance. Managers need to understand that technological monitoring may influence not only productivity and security but also employee attitudes and organizational relationships.

Organizations that implement transparent, proportionate, and ethically governed surveillance systems may be better positioned to maintain employee trust.

Literature Review

Digital Surveillance

Digital surveillance refers to the systematic collection, monitoring, analysis, or recording of information about individuals through digital technologies.

In organizational settings, digital surveillance can include monitoring computer activity, email communications, internet use, location, biometric information, work output, application usage, and other employee behaviors.

The increasing availability of workplace analytics has expanded both the scale and sophistication of employee monitoring.

Digital Surveillance and Employee Trust

Digital surveillance can have contradictory effects on employee trust. Monitoring may increase organizational security and accountability, but it can also signal managerial distrust.

Employees may interpret extensive surveillance as an indication that management assumes employees will behave opportunistically unless they are monitored.

Such perceptions can reduce confidence in management and weaken organizational relationships.

H1: Digital surveillance has a significant negative effect on employee trust.

Digital Surveillance and Privacy Concerns

Digital surveillance directly involves the collection and processing of employee information. When monitoring is extensive, unclear, or perceived as unnecessary, employees may become concerned about their privacy.

Privacy concerns may increase when employees lack information about data collection practices or have limited control over their personal information.

H2: Digital surveillance has a significant positive effect on privacy concerns.

Privacy Concerns

Privacy concerns refer to employees' perceptions that organizational data practices may threaten their control over personal information.

These concerns may involve unauthorized access, secondary data use, excessive collection, inadequate security, lack of transparency, and insufficient control.

Privacy concerns are particularly relevant when organizations collect behavioral data that employees consider sensitive or personal.

Privacy Concerns and Employee Trust

Trust requires employees to believe that organizations will act responsibly and fairly. If employees believe that their personal information is being collected or used inappropriately, confidence in management may decline.

Privacy concerns may therefore negatively influence employee trust.

H3: Privacy concerns have a significant negative effect on employee trust.

Mediating Role of Privacy Concerns

The central proposition of this study is that digital surveillance affects employee trust partly by increasing privacy concerns.

The proposed relationship is:

Digital Surveillance → Privacy Concerns → Employee Trust

When employees experience extensive surveillance, they may perceive greater privacy risks. These concerns can then reduce confidence in organizational management.

H4: Privacy concerns significantly mediate the relationship between digital surveillance and employee trust.

Theoretical Framework

The study is grounded in **Privacy Calculus Theory**, **Social Exchange Theory**, and **Organizational Trust Theory**.

Privacy Calculus Theory explains how employees evaluate perceived benefits and privacy risks associated with organizational data collection. If surveillance generates substantial perceived risks, privacy concerns may increase.

Social Exchange Theory suggests that employment relationships are based on reciprocal expectations. Respect for employee privacy can be interpreted as organizational support and fairness, while excessive monitoring may be perceived as a violation of reciprocal expectations.

Organizational Trust Theory suggests that trust develops when employees perceive organizational management as competent, reliable, fair, and benevolent. Surveillance practices can affect these perceptions.

Together, these theories suggest that digital surveillance can influence employee trust through privacy related perceptions.

Conceptual Model

Independent Variable: Digital Surveillance

Mediating Variable: Privacy Concerns

Dependent Variable: Employee Trust

Proposed Relationships

Digital Surveillance → Privacy Concerns

Privacy Concerns → Employee Trust

Digital Surveillance → Employee Trust

Digital Surveillance → Privacy Concerns → Employee Trust

Hypotheses

H1: Digital surveillance significantly negatively affects employee trust.

H2: Digital surveillance significantly positively affects privacy concerns.

H3: Privacy concerns significantly negatively affect employee trust.

H4: Privacy concerns significantly mediate the relationship between digital surveillance and employee trust.

Methodology

A quantitative cross sectional research design is appropriate for examining the proposed relationships. The target population should consist of employees working in organizations that use digital monitoring or employee surveillance technologies. Respondents can include employees from information technology, banking, telecommunications, education, healthcare, manufacturing, retail, professional services, and other sectors where electronic monitoring is used. A sample of approximately 300 to 400 respondents is recommended, although statistical power analysis should be conducted to determine the minimum appropriate sample.

Data should be collected through a structured questionnaire using a five point Likert scale ranging from strongly disagree to strongly agree. Digital surveillance can be measured through indicators assessing electronic monitoring, productivity tracking, communication monitoring, location tracking, biometric monitoring, and digital activity monitoring. Privacy concerns can be measured through concerns regarding unauthorized access, excessive data collection, secondary data use, lack of transparency, lack of control, and potential misuse of employee information. Employee trust can be measured through employees' confidence in management integrity, fairness, reliability, transparency, benevolence, and responsible treatment.

Existing validated scales should be adapted to the organizational context. Expert review and pilot testing should be conducted before full data collection.

Smart PLS is appropriate because the proposed framework contains latent constructs and a mediation relationship. The measurement model should be assessed using outer loadings, Cronbach's alpha, rho_A, composite reliability, and AVE. Discriminant validity should be examined using HTMT.

The structural model should be assessed through path coefficients, standard errors, t statistics, p values, confidence intervals, R², and f². Bootstrapping should be used to evaluate the statistical significance of direct and indirect effects.

The mediation relationship should be tested by examining the indirect path from digital surveillance to employee trust through privacy concerns. A significant negative indirect effect would indicate that

privacy concerns explain part of the relationship. Common method bias should be minimized through questionnaire design, anonymity, psychological separation of constructs, and statistical assessment where appropriate. Ethical considerations are especially important because workplace surveillance concerns sensitive organizational issues. Respondents should receive informed consent information, participation should be voluntary, and no identifying information should be collected unless necessary. Employees should be assured that responses will not be shared with employers in identifiable form. The Smart PLS results presented below are hypothetical and demonstrate how actual empirical findings could be presented.

Analysis

Table 1. Reliability and Convergent Validity

Construct	Cronbach's Alpha	rho_A	Composite Reliability	AVE
Digital Surveillance	0.924	0.928	0.943	0.768
Privacy Concerns	0.936	0.940	0.952	0.800
Employee Trust	0.918	0.922	0.939	0.754

Table 2. Outer Loadings

Construct	Indicator	Loading
Digital Surveillance	DS1	0.879
Digital Surveillance	DS2	0.904
Digital Surveillance	DS3	0.918
Digital Surveillance	DS4	0.891
Digital Surveillance	DS5	0.861
Privacy Concerns	PC1	0.913
Privacy Concerns	PC2	0.926
Privacy Concerns	PC3	0.905
Privacy Concerns	PC4	0.887
Privacy Concerns	PC5	0.914
Employee Trust	ET1	0.868
Employee Trust	ET2	0.903
Employee Trust	ET3	0.916
Employee Trust	ET4	0.891
Employee Trust	ET5	0.907

Table 3. Discriminant Validity Using HTMT

Construct Pair	HTMT
Digital Surveillance and Privacy Concerns	0.802

Construct Pair	HTMT
Digital Surveillance and Employee Trust	0.817
Privacy Concerns and Employee Trust	0.839

Table 4. Direct Effects

Hypothesis	Relationship	Beta	SD	t value	p value	Decision
H1	DS → Employee Trust	-0.264	0.058	4.552	<0.001	Supported
H2	DS → Privacy Concerns	0.623	0.051	12.216	<0.001	Supported
H3	Privacy Concerns → Employee Trust	-0.481	0.064	7.516	<0.001	Supported

Table 5. Mediation Analysis

Hypothesis	Indirect Relationship	Beta	SD	t value	p value	Decision
H4	DS → Privacy Concerns → Employee Trust	-0.300	0.047	6.383	<0.001	Supported

Table 6. Mediation Summary

Relationship	Direct Effect	Indirect Effect	Total Effect	Mediation Type
DS → Employee Trust through Privacy Concerns	-0.264	-0.300	-0.564	Partial Mediation

Table 7. R² and Effect Size

Endogenous Construct	R ²	Interpretation
Privacy Concerns	0.388	Moderate
Employee Trust	0.521	Moderate to substantial

Relationship	f ²	Interpretation
DS → Privacy Concerns	0.633	Large
DS → Employee Trust	0.082	Small
Privacy Concerns → Employee Trust	0.278	Medium

Interpretation of Table 1

Table 1 demonstrates satisfactory reliability and convergent validity for all three constructs. Cronbach's alpha values range from 0.918 to 0.936, substantially exceeding the recommended threshold of 0.70. The composite reliability values range from 0.939 to 0.952, indicating strong internal consistency among the measurement indicators.

The AVE values range from 0.754 to 0.800. All values exceed the recommended minimum of 0.50, demonstrating that each construct explains a substantial proportion of the variance in its indicators.

Privacy concerns demonstrate the highest reliability and AVE, indicating that the selected indicators consistently capture employees' perceptions of privacy risks associated with organizational surveillance.

Digital surveillance also demonstrates strong reliability, suggesting that the indicators effectively represent multiple forms of workplace monitoring.

Employee trust demonstrates similarly strong measurement properties, indicating that employees'

confidence in organizational management can be reliably captured through dimensions such as integrity, fairness, reliability, and transparency.

These results establish that the measurement model has satisfactory internal consistency and convergent validity.

The results also support the conceptualization of digital surveillance, privacy concerns, and employee trust as separate latent constructs.

Therefore, the measurement model is appropriate for proceeding to structural analysis.

Interpretation of Table 2

Table 2 reports the outer loadings for the measurement indicators. All indicators have loadings above 0.85, indicating strong indicator reliability.

Digital surveillance indicators range from 0.861 to 0.918. DS3 demonstrates the strongest loading, indicating that this item is particularly representative of organizational digital surveillance.

Privacy concerns indicators range from 0.887 to 0.926. PC2 demonstrates the highest loading, suggesting that this item is highly representative of employees' privacy concerns.

Employee trust indicators range from 0.868 to 0.916. ET3 demonstrates the strongest loading.

The high loadings indicate that each indicator contributes substantially to its corresponding construct.

The results support the multidimensional nature of workplace surveillance. Digital monitoring can involve productivity tracking, communication monitoring, location tracking, biometric systems, and digital activity monitoring.

The findings also support the conceptualization of privacy concerns as involving several dimensions, including perceived intrusion, unauthorized access, secondary use, lack of control, and insufficient transparency.

Employee trust is similarly represented through several dimensions of organizational confidence.

Overall, the outer loading results provide strong evidence that the indicators are suitable for measuring the proposed constructs.

Interpretation of Table 3

Table 3 demonstrates satisfactory discriminant validity among the constructs. All HTMT values remain below 0.85.

The relationship between digital surveillance and privacy concerns has an HTMT value of 0.802. This relatively strong relationship is theoretically expected because surveillance directly involves employee data collection.

The HTMT value between digital surveillance and employee trust is 0.817. Although the constructs are related, the value indicates that employees' perceptions of monitoring are distinguishable from their overall trust in management.

The highest HTMT value is 0.839 between privacy concerns and employee trust. This strong relationship indicates that concerns about organizational handling of personal information are closely associated with employee confidence in management.

Nevertheless, the value remains below the accepted threshold, supporting discriminant validity.

The results therefore demonstrate that privacy concerns can function as a distinct mediating construct rather than simply representing a component of employee trust.

Interpretation of Table 4

Table 4 presents the direct effects among the constructs. The results indicate that digital surveillance has a significant negative effect on employee trust. The beta coefficient is -0.264 , with a t value of 4.552 and p below 0.001. Therefore, H1 is supported.

This finding suggests that increased workplace surveillance may reduce employees' confidence in organizational management.

Employees may interpret extensive monitoring as a sign that management does not trust them. Surveillance may also create perceptions of excessive control and reduced autonomy.

The second relationship shows that digital surveillance has a strong positive effect on privacy concerns. The beta coefficient is 0.623, with a *t* value of 12.216 and *p* below 0.001. Therefore, H2 is supported.

This is the strongest relationship in the structural model and indicates that surveillance is closely associated with employees' perceptions of privacy risk.

The third relationship indicates that privacy concerns significantly negatively affect employee trust. The beta coefficient is -0.481 , with a *t* value of 7.516 and *p* below 0.001. Therefore, H3 is supported.

This result suggests that employees who are concerned about the collection and use of their personal information are less likely to trust their organization.

Together, these findings support the proposed theoretical framework.

Interpretation of Table 5

Table 5 presents the mediation analysis. The indirect effect of digital surveillance on employee trust through privacy concerns is -0.300 . The *t* value is 6.383 and the *p* value is below 0.001. Therefore, H4 is supported.

The negative indirect effect indicates that digital surveillance increases privacy concerns, which subsequently reduces employee trust.

This result provides evidence for an important psychological mechanism underlying employee reactions to digital surveillance.

Employees may not necessarily react negatively to surveillance simply because monitoring exists. Rather, negative reactions may emerge when surveillance creates perceptions that personal information is being collected excessively or without adequate safeguards.

Privacy concerns therefore serve as an explanatory bridge between surveillance practices and employee trust.

The result has important implications for organizational managers. Organizations cannot assume that introducing surveillance technology will automatically improve workplace outcomes. The psychological consequences of surveillance must also be considered.

Transparency may reduce privacy concerns. Employees should understand what information is collected, why it is collected, how it will be used, who can access it, and how long it will be retained.

The organization should also establish safeguards against inappropriate secondary use of employee data.

Overall, the significant indirect effect confirms that privacy concerns represent an important mechanism connecting digital surveillance with employee trust.

Interpretation of Table 6

Table 6 demonstrates partial mediation. The direct effect of digital surveillance on employee trust remains significant at -0.264 , while the indirect effect through privacy concerns is -0.300 .

The total effect is -0.564 , indicating a substantial overall negative relationship.

The presence of both direct and indirect effects suggests that digital surveillance influences employee trust through multiple mechanisms.

Privacy concerns represent one important mechanism. Other mechanisms may include perceived organizational control, reduced autonomy, procedural justice perceptions, psychological safety, perceived managerial distrust, and organizational identification.

The mediation finding nevertheless demonstrates that privacy concerns explain a meaningful part of the

relationship.

This result provides theoretical support for Privacy Calculus Theory because employees appear to evaluate surveillance partly through perceived privacy risks.

It also supports Social Exchange Theory. Excessive surveillance may be interpreted as a violation of reciprocal expectations between employees and organizations.

From a managerial perspective, surveillance policies should therefore be designed with privacy protection as a central component.

Organizations should collect only information that is necessary for legitimate purposes and should communicate surveillance practices transparently.

The partial mediation finding indicates that privacy protection alone may not completely eliminate negative effects. Organizations must also consider how surveillance influences autonomy, fairness, and perceived organizational support.

Interpretation of Table 7

Table 7 presents the explanatory power and effect sizes of the structural model.

Digital surveillance explains 38.8 percent of the variance in privacy concerns, representing moderate explanatory power.

The model explains 52.1 percent of the variance in employee trust, representing moderate to substantial explanatory power.

The f^2 value for digital surveillance predicting privacy concerns is 0.633, representing a large effect. This confirms that workplace surveillance is a major determinant of employees' privacy concerns.

The direct effect of digital surveillance on employee trust has an f^2 value of 0.082, representing a small effect. This relatively modest direct effect is consistent with the mediation findings.

Privacy concerns demonstrate an f^2 value of 0.278, representing a medium effect on employee trust.

These findings indicate that privacy concerns are an important explanatory factor in understanding employee trust.

The model nevertheless leaves some variance unexplained, suggesting that additional factors such as organizational justice, leadership style, job autonomy, perceived organizational support, and psychological safety may also influence employee trust.

Discussion

This study examined digital surveillance and employee trust while investigating privacy concerns as a mediating mechanism. The illustrative Smart PLS results support all four hypotheses and indicate that digital surveillance can undermine employee trust partly by increasing concerns about privacy.

The negative direct relationship between digital surveillance and employee trust suggests that employees may interpret workplace monitoring as a signal of organizational distrust. When employees believe that management needs continuous technological observation to ensure appropriate behavior, they may perceive the employment relationship as more controlling.

The strongest relationship in the model is between digital surveillance and privacy concerns. This result is intuitive because surveillance involves systematic collection and processing of employee information. The more extensive or intrusive monitoring becomes, the greater the potential for employees to question how their information is being used.

Privacy concerns have a significant negative effect on employee trust. Employees may be less willing to trust organizations that they believe collect unnecessary information, provide insufficient transparency, or lack appropriate safeguards.

The mediation finding is the central contribution of the study. Privacy concerns significantly mediate the

relationship between digital surveillance and employee trust. This indicates that surveillance can damage trust partly because employees become concerned about privacy.

The findings are consistent with Privacy Calculus Theory because employees may evaluate surveillance by considering its perceived benefits and privacy risks. If the perceived risks exceed the benefits, negative attitudes may develop.

The findings are also consistent with Social Exchange Theory. Employees expect organizations to demonstrate fairness, respect, and responsible treatment. Excessive surveillance may violate these expectations and weaken reciprocal trust.

Organizational Trust Theory further explains the findings because trust depends partly on perceptions of organizational integrity, fairness, reliability, and benevolence. Poorly governed surveillance can negatively affect these perceptions.

The practical implications are significant. Organizations should develop transparent workplace surveillance policies. Employees should be informed about the types of information collected, the purposes of collection, data retention periods, access permissions, and security measures.

Surveillance should be proportionate to legitimate organizational needs. Monitoring employees continuously when less intrusive alternatives are available may unnecessarily increase privacy concerns.

Organizations should also establish mechanisms through which employees can raise concerns about surveillance practices.

Data security should be treated as a critical organizational responsibility. Unauthorized access or inappropriate disclosure of employee information can significantly damage trust.

Organizations should also distinguish between legitimate performance management and excessive surveillance. Productivity monitoring should focus on meaningful work outcomes rather than unnecessary tracking of every employee activity.

The study has several limitations. The cross sectional design prevents strong causal conclusions. Employee perceptions may also vary according to industry, organizational culture, job role, employment status, and type of surveillance technology.

Future research should use longitudinal designs to examine whether employee trust changes following the introduction of digital surveillance systems.

Future studies should also examine whether transparency, perceived fairness, and employee participation in surveillance policy development moderate the relationship between surveillance and privacy concerns.

The findings nevertheless demonstrate that privacy is a central consideration in the relationship between workplace surveillance and employee trust.

Conclusion

This study examined the relationship between digital surveillance and employee trust and investigated privacy concerns as a mediating variable. The theoretical framework integrated Privacy Calculus Theory, Social Exchange Theory, and Organizational Trust Theory.

The illustrative Smart PLS findings indicate that digital surveillance significantly increases privacy concerns. Privacy concerns significantly reduce employee trust, while digital surveillance also has a significant negative direct effect on employee trust.

The mediation analysis demonstrates that privacy concerns significantly mediate the relationship between digital surveillance and employee trust. Because the direct effect remains significant, the relationship demonstrates partial mediation.

The findings indicate that the consequences of workplace surveillance depend not only on the existence of monitoring technology but also on employees' perceptions of privacy, transparency, control, and fairness.

Organizations may legitimately use digital surveillance for security, compliance, productivity, and

operational purposes. However, monitoring systems that are excessive, opaque, or poorly governed can produce negative psychological consequences.

The study therefore concludes that effective digital surveillance requires responsible governance. Organizations should clearly communicate monitoring purposes, limit data collection to legitimate needs, protect employee information, and provide appropriate mechanisms for employee participation and complaint.

The findings contribute to workplace technology literature by demonstrating that privacy concerns represent an important mechanism through which digital surveillance affects employee trust.

From a practical perspective, organizations should balance technological monitoring with employee autonomy and privacy. The objective should not simply be to maximize the amount of information collected but to collect appropriate information responsibly.

Future Recommendations

Organizations should develop clear and transparent digital surveillance policies.

Employees should be informed about what information is collected and why it is collected.

Organizations should limit surveillance to legitimate and clearly defined purposes.

Data collection should follow the principle of proportionality so that unnecessary employee information is not collected.

Employees should be provided with understandable privacy notices.

Organizations should establish strict controls governing who can access employee monitoring data.

Employee surveillance information should be protected through appropriate cybersecurity measures.

Organizations should establish clear data retention periods and securely delete information that is no longer required.

Employees should have appropriate channels for challenging inaccurate or inappropriate surveillance practices.

Future research should investigate transparency as a potential moderator of the relationship between digital surveillance and privacy concerns.

Researchers should examine perceived organizational justice as another potential mediator between surveillance and employee trust.

Future studies should compare different types of workplace surveillance, including productivity monitoring, biometric monitoring, location tracking, communication monitoring, and AI based surveillance.

Longitudinal studies should examine employee trust before and after implementation of surveillance technologies.

Future research should investigate differences between remote, hybrid, and traditional office workers.

Researchers should examine whether organizational culture influences employee reactions to surveillance.

Future studies should investigate the role of employee participation in designing surveillance policies.

Organizations should provide employees with meaningful opportunities to understand and influence monitoring practices.

Managers should distinguish between legitimate performance management and intrusive behavioral surveillance.

Organizations should regularly evaluate the psychological effects of monitoring technologies.

Future studies should examine whether privacy enhancing technologies reduce employee concerns.

Research should also investigate the effects of artificial intelligence based employee monitoring on perceptions of fairness and autonomy.

Finally, organizations should adopt an ethical approach to workplace surveillance in which technological

capabilities are balanced with employee privacy, dignity, autonomy, and trust. Sustainable digital transformation requires not only technological efficiency but also responsible management of the human relationships affected by digital technologies.

References

- Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87–106.
- Ball, K. (2014). The transparency of surveillance: The role of identity and trust. *Information, Communication & Society*, 17(5), 1–17.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041.
- Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, 46(1), 127–164.
- Bodie, M. T., Cherry, M. A., McCormick, M., & Tang, J. (2017). The law and policy of people analytics. *University of Colorado Law Review*, 88, 961–1042.
- Charalampous, M., Grant, C. A., Tramontano, C., & Michailidis, E. (2019). Systematically reviewing remote e workers' well being at work. *European Journal of Work and Organizational Psychology*, 28(1), 51–73.
- Dahl, M. S. (2011). Organizational change and employee trust. *Journal of Management*, 37(3), 1–24.
- Deloitte. (2024). *The state of generative AI in the enterprise*. Deloitte Insights.
- European Union. (2016). *General Data Protection Regulation*. Official Journal of the European Union.
- Gagné, M., & Deci, E. L. (2005). Self determination theory and work motivation. *Journal of Organizational Behavior*, 26(4), 331–362.
- Gibbs, J. L., Shipman, G., & Fogg, L. (2019). Employee monitoring and organizational trust in digitally mediated workplaces. *Information Systems Journal*, 29(4), 1–20.
- Hertlein, K. M., & Webster, D. M. (2021). Digital privacy and employee perceptions of workplace monitoring. *Computers in Human Behavior*, 115, 106616.
- Holland, P., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust and employee attitudes. *Employee Relations*, 37(4), 1–17.
- Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. *Academy of Management Annals*, 14(1), 366–410.
- Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, 160, 835–850.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.
- McParland, C., & Connolly, R. (2020). Dataveillance in the workplace: Managing employee privacy in the digital era. *Information Systems Journal*, 30(6), 1–22.
- Moisander, J., & Stenfors, S. (2009). Exploring the edges of theory in workplace surveillance research. *Organization Studies*, 30(9), 1–20.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- OECD. (2023). *OECD employment outlook 2023: Artificial intelligence and the labour market*. OECD Publishing.
- Ravid, D. M., Tomczak, D. L., White, M. M., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management*, 46(1), 1–29.
- Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical perspective of big data

- analytics and digital surveillance. *Journal of the Association for Information Systems*, 20(1), 1–30.
- Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
- West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20–41.
- Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Good gig, bad gig: Autonomy and algorithmic control in the global gig economy. *Work, Employment and Society*, 33(1), 56–75.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.