ACADEMIA International Journal for Social Sciences
Volume 4, Issue 1, 2025 ISSN-L (Online): 3006-6638

Digital Surveillance and Privacy Concerns the Changing Dynamics of Trust in Modern Societies: A Mediation Moderation Model

Taimoor Tabasum
taimoortabasum1414@gmail.com
Department of Sociology, University of Sargodha, Pakistan
Saima Iram
saimairamuos@gmail.com
Department of Sociology, Thal University Bhakkar, Pakistan
Sakhawat Ali
sakhawatmuradi52@gmail.com
Department of Sociology, Karakorum International University
Mishal Akhtar
mishalbaloch1311@gmail.com
Department of Sociology, Thal University Bhakkar, Pakistan
Musharaf Hussain
musharafhussain763@gmail.com
Department of Sociology, University of Sargodha Pakistan
Corresponding Author: * **Taimoor Tabasum** taimoortabasum1414@gmail.com

Received: 02-01-2025 **Revised:** 29-01-2025 **Accepted:** 11-02-2025 **Published:** 02-03-2025

ABSTRACT

In the digital era of transformation, surveillance technologies have reformed the texture of modern societies and initiated serious questions around privacy and trust in institution and modern societies. This research explores the complex linkages among digital surveillance, concerns for privacy, regulatory environment, and institutional public trust using the mediation-moderation framework. Based on the Communication Privacy Management (CPM) Theory, the research conceptualizes how individuals judge and navigate intimate information while perpetually facing digital surveillance. Utilizing a quantitative research approach, data were collected from 220 Pakistani and Chinese university students through structured online questionnaires developed by using validated Measurement Scales. The Correlation result indicates that these is negative impact of Digital Surveillance on the Trust in modern Societies. Mediation analysis using PROCESS Macro (Model 4) also supported that digital surveillance has a strong negative effect on public trust (β = –0.33, p = .001), with privacy concern as a significant mediator (indirect effect = –0.21, 95% CI [–0.31, –0.12]). In addition, analysis of moderation established that regulatory framework act as buffers to this impact since the interaction term was found to be significant (β = 0.18, p =.003), showing weaker regulatory environments weaken trust eroded by surveillance. The findings accentuate that concerns about privacy sharpen distrust in environments with heavy surveillance, but adequate regulatory frameworks block this effect. This work makes theoretical contributions by applying CPM Theory in institutional settings and provides policy suggestions for policymakers and digital platform engineers. It stresses the need for open, transparent data governance in order to revive and maintain confidence in the era of the internet.

Keywords: *Digital Surveillance; Privacy Concern; Trust in Modern Societies; Regulatory Framework*

INTRODUCTION

The surveillance abilities of modern technology during the digital age have transformed social arrangements and rules and privacy concepts. Digital surveillance systems managed to reduce cybercrime and provide personalized services through capabilities which came at a cost of significant conflicts for privacy rights together with civil liberties and public trust (Zuboff, 2023). Surveillance research initiatives started due to rising academic interest about institutional-technological trust links during the adoption and privacy concerns of digital infrastructure. Known privacy issues must guide modern communities who want to establish a fair monitoring system that links trust with digital surveillance.

Modern societies need to understand digital surveillance effects on trust because researchers have investigated four central variables in their detailed research. Governmental repositories together with organizations and corporations execute digital surveillance when they monitor online activities to collect personal information (Lyon, 2018). The research examines how digital surveillance systems generate particular effects on public understanding and societal trust creation. Social cohesion functions through trust because it sustains democratic decision-making simultaneously encouraging citizens to unite as groups. The normal operation of contemporary societies requires complete trust placed in their institutions as well as corporations and online platforms (Neto, 2023). People feel concerned about their privacy after discovering their personal information is captured without permission. The degree to which people worry about protecting their personal data acts as a mediator that affects how digital surveillance impacts their trust (Smith et al., 2011). People who think their privacy faces danger will start to lose faith in government institutions as well as corporations and organizations. The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) together with other regulatory frameworks aim to protect individual rights by establishing regulations for digital surveillance practices (Solove, 2012). The regulations serve to decrease trust-related consequences of digital surveillance by guaranteeing privacy rights and establishing clear monitoring practices. The research provides important insights about digital surveillance impacts on trust through privacy concerns by analyzing regulatory frameworks that play a moderating role in this relationship. The exploration of these dynamic relationships represents an essential requirement for political leaders and business organizations along with civil society groups to create security privacy balancing systems.

Digital surveillance research continuously increases in academia despite scientists needing more insight into privacy and surveillance relationships with trust foundational elements. Academic research mainly investigates three areas of digital surveillance: governmental surveillance practices as studied by (Van Dijck, 2014), and data sharing ethical dilemmas according to (Richards, 1934), and public attitudes toward online monitoring as explained by (Taylor, 2017). Academic research about privacy-related networked relationship mediation and regulatory trust-level effects in published studies is insufficient. Research evidence confirms that digital transparency and regulatory oversight create positive outcomes according to (Bennett & Raab, 2017), yet researchers have not established full models linking these aspects together. This investigation assesses trust dissolution from digital monitoring through privacy assessment and contains regulatory components that minimize privacy threats. Modern digital trust patterns lack sufficient research-based understanding which allows this investigation to deliver specific data about modern trust behavior in digital environments.

Multiple key variables with influencing conditions help the research analyze trust-based interactions between modern societies and digital surveillance systems. The research investigates how surveillance affects trust directly together with assessing privacy risks that develop in these trust-based relationships. Research studies have identified how rules and regulations change both trust perceptions and privacy concerns of individuals. Results from this investigation lead both authorities and key stakeholders to develop proper security measures that simultaneously protect privacy standards and build public trust. The research dataset establishes basic principles to achieve digital system transparency as well as accountability while enhancing worldwide comprehension of governance security and ethical data management procedures.

Features of digital surveillance technology advance rapidly which leads modern societies to fear major privacy violations. Organizations and governments use data analysis activities intensively to collect substantial personal information that results in ethical challenges for data stewardship. National security surveillance systems and economic efficiency instruments generate unintended effects which decrease institutional trust from people. Inability to manage data processing by individuals results in deepening tensions that exist between citizens and government agencies as well as between citizens and corporate standards about ethical conduct. Citizens develop more distrust because of weak privacy regulations which fail to protect their privacy rights. Scientists need to understand the intricate relationship between digital

surveillance methods and privacy concerns and trust because doing so provides necessary information for making policies that maintain both ethical and technological balance. A mediation-moderation model within this research explores the effects which privacy concerns and regulatory systems have on digital social trust elements.

Hypothesis Development

Today modern societies experience growing digital surveillance practices that monitor people's online activities together with their personal data collection. Surveillance activities commonly result in decreasing public trust since people become knowledgeable about continuous monitoring of their data (Lyon, 2018). People who detect violations of their privacy feelings become vulnerable and start to distrust both public institutions and private companies which collect data (Zuboff, 2023). According to recent studies people started doubting social institutions along with questioning their intentions when surveillance techniques invade their liberties (Fuchs, 2019).

H1: Digital Surveillance negatively effects the Trust in Modern Societies

The protection of personal information acts as a major factor which affects how individuals respond to digital surveillance measures. The concerns about personal data security together with autonomy increase for people who feel their privacy is threatened by digital surveillance (Solove, 2010). The increased awareness about privacy breaches generates skepticism towards authorities performing surveillance thereby reducing trust in both government agencies and corporate bodies (Fano, 1968). Individuals develop increasing wariness about data management practices which causes them to lose trust in governing systems (Krasnova et al., 2012).

H2: Privacy Concern mediates the link between Digital Surveillance and Trust in Modern Societies.

Public trust between individuals depends heavily upon the presence of strict regulatory systems which protect privacy in our modern societies. Aliment of strong privacy laws and data protection regulations leads people to put their trust in responsible data management practices for their private information (Tufekci, 2015). Modern privacy regulations achieve three objectives: they promote transparency, maintain accountability and protect individual rights which helps decrease digital surveillance-related fears (Rodrigues et al., 2023). Weaker or less consistent privacy regulations worsen privacy risks because people believe their data is exposed to possible misuse or exploitation (Barth & De Jong, 2017).

H3: Regulatory Framework moderates the link between Privacy Concern and Trust in Modern Societies.

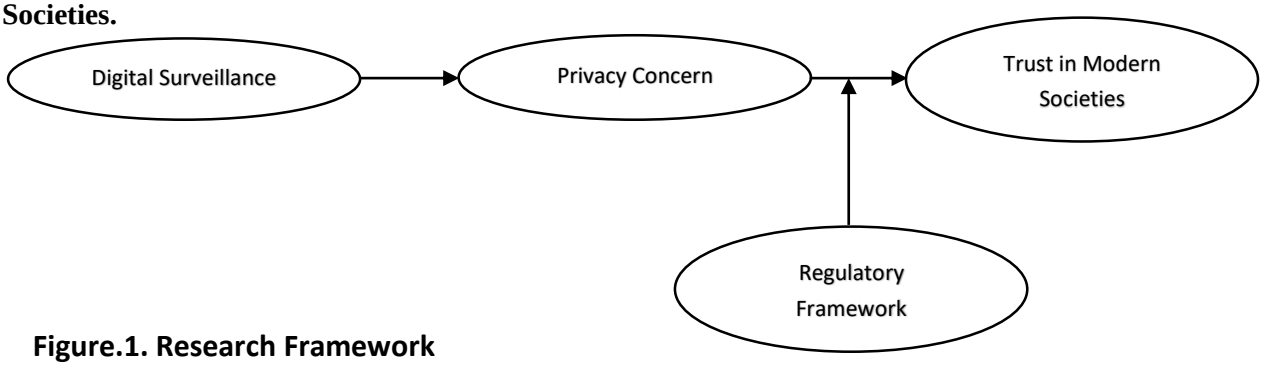

Figure.1. Research Framework

LITERATURE REVIEW AND THEORETICAL FOUNDATION

The fundamental role of digital surveillance in present-day governance and organizational security results from advanced artificial intelligence (AI) and big data and cybersecurity technology developments (Zuboff, 2023). The government together with corporations utilizes digital surveillance capabilities for both crime prevention and national security functions as well as marketing purposes. The extensive implementation of surveillance systems triggers privacy violations combined with major ethical worries (Mannan, 2025). People commonly feel powerless over their personal data collection through both data gathering and facial identification and predictive analysis mechanisms.

People fear unauthorized access of private data and data breaches as well as potential misuse of personal information thus creating privacy concerns (Acquisti et al., 2015). The analysis shows digital surveillance monitoring produces a chilling effect because people modify their online actions because they fear observation (Solove, 2021). Privacy issues create major trust deterioration between people and government institutions and corporate bodies while also affecting people's Digital platform usage (Smith et al., 2011).
The core essence of trust operates as an essential component in digital spaces while it determines interpersonal relations between people and institutions and business entities. The trust in digital surveillance includes institutional trust regarding government entities and corporations alongside interpersonal trust toward online individuals (Bodó, 2021). Public trust depends heavily on the way data operations are made transparent and organizations follow privacy laws (Bednar & Sadok, 2024). Trust functions as a coordinating variable which links privacy concerns and personal information sharing practices (Mutimukwe et al., 2020). People become less concerned about digital surveillance when they believe data governance has strong transparency along with accountability measures in place. When surveillance goes beyond user-approved limits it breaks trust which makes individuals disengage and resist (Schneier, 2015). Various research papers demonstrate how trust functions as a connecting element to bridge relationships between digital engagement and privacy issues (Dinev et al., 2015). Those who trust institutions accept surveillance measures since they view these measures as security safeguards (Martin, 2019). Trust acts as a mediator in these relationships while its effect depends on regulatory factors and how transparent data protection standards are as well as individual understanding of these standards (Bélanger & Crossler, 2011). Public trust moderation found its essential implementation by the European Union through their adoption of GDPR regulations which established firm data protection standards according to (Tikkinen-Piri et al., 2018). Users determine how they feel about surveillance methods based on the data privacy policies and ethical AI standards that corporations establish (Dhirani et al., 2023). Data knowledge functions as a trust-controlling element because people with privacy law comprehension experience decreased surveillance anxiety according to (Kleynhans et al., 2022).

Theoretical Foundation: (Communication Privacy Management Theory).

Communication Privacy Management Theory (CPM) functions as theoretical frameworks to support this research. The study derives its most suitable theoretical framework from Communication Privacy Management (CPM) Theory which (Petronio, 2002). The theoretical framework provides a comprehensive model which enables us to assess both border management and adjustment practices of personal data by people during digital surveillance days. According to CPM theory each person maintains power over their personal information data while serving as the sole controller of exposure decisions for the data. Digital surveillance without authorization inspires people to think of it as a violation of personal boundaries regarding privacy. The unauthorized access to their data triggers privacy concerns because people fear their data could be abused or locked off indefinitely and they lose ability to protect their confidential items. Social trust in the modern world faces escalating worries because individuals do not trust government organizations together with technology businesses and regulatory agencies. The CPM theory adopts societal regulations about privacy information transfer in the same way that regulatory oversight protects research data privacy. A clear regulatory structure works as an obstacle-linked system to allow people experiencing privacy security through digital surveillance. Legitimate surveillance policies serve as a moderating influence by minimizing privacy issues due to surveillance practices because they supply legal backing to such procedures. The analysis of surveillance-trust links through privacy concerns becomes possible because of CPM theory and gain insight into regulatory body impacts on trustworthiness and privacy. Public trust regarding digital surveillance depends on privacy concerns as explained by Communication Privacy Management Theory alongside regulatory frameworks which affect this connection.

METHODOLOGY

Data Collection and Sample

The study employed quantitative and cross-sectional research design to investigate relationships between digital surveillance and trust in modern societies, privacy concerns as mediator and regulatory authority as

a moderator. The target population was Public and Private University students of Pakistan and China. Stratified random sampling techniques were implemented to attain proper representation of diverse population segments especially for age brackets and regional distributions. A sample of 220 participants was selected to analyze the mediation-moderation model since this number offered sufficient power for robust statistical outcomes. Online surveys served as the chosen method for data collection because they provided convenient and cost-effective research that allowed researcher to reach broad audiences. The survey instrument employed a structured questionnaire which incorporated Likert scale items to evaluate the four essential constructs including digital surveillance followed by privacy concerns and Regulatory Framework and trust in modern societies. A preliminary study or Pilot study comprising 30-50 participants evaluated the research tool before the main data collection to validate its clarity and accuracy alongside reliability and validity. Analysis of collected data involved the use of SPSS and AMOS Software. Data analysis proceeded through multiple stages. Initially descriptive statistics described participant demographics characteristics. Confirmatory Factor Analysis (CFA) utilized to validate the measurement model and ensure the accuracy of digital surveillance, privacy concerns, trust, and regulatory framework scales. Research utilized correlation analysis methods to determine relationships and their degrees between all variables. The Process Macro (Model 4) in SPSS ran mediation analysis to determine how privacy concerns functioned as a mediator between digital surveillance and trust in modern societies. The mediation effect received testing through bootstrapping analysis that produced confidence intervals to determine the significance of mediating pathways. The research also included moderation analysis to study how different regulatory framework strengths affect the relationship between privacy concerns and Trust in modern societies. The various analyses produced thorough findings about the relationships between digital surveillance practices and privacy concerns and regulatory frameworks within trust systems of contemporary societies.

Scale Measurement

The study uses validated measurement scales to evaluate its core variables. Digital Surveillance (Independent Variable) was measured through a Digital Surveillance Concerns Scale which adapted seven items rated on a 5-point Likert scale from (Dinev et al., 2008). We utilize the Generalized Social Trust Scale to assess Trust in Modern Societies (Dependent Variable) by administering seven items using a 5-point Likert scale according to the work of (Bélanger & Carter, 2008; Yamagishi & Yamagishi, 1994). The assessment of Privacy Concerns (Mediator) utilizes the Internet Users' Information Privacy Concerns (IUIPC) Scale which contains ten items with a 5-point Likert scale developed by (Malhotra et al., 2004). The Perceived Regulatory Protection Scale is used to measure the Regulatory Framework (Moderator) while adopting seven items from (Belanger & Carter, 2012; Xu et al., 2009). These items utilize a 5-point Likert scale. Multiple research-based scales achieve both accuracy and reliability of measurement to analyze the interrelationships between digital surveillance together with trust and privacy concerns and regulatory frameworks.

RESULT

The Table.1. Demonstrates that study participants have diverse demographic characteristics which support the robustness and general applicability of study findings. A significant number of 60.9% of surveyed individuals identified as female in a total sample of 220 participants and the remaining 39.1% included males. The skewed participant gender split allows us to understand distinctive surveillance perception patterns between men and women during situations when privacy concern levels run high for women. The survey participants who achieved an undergraduate level of education represented the highest demographic group comprising 49% while graduate and postgraduate degree holders amounted to 32.7% and 18.1% respectively. The study benefits from educational diversity which allows students from different backgrounds to provide complex viewpoints about digital governance approaches and surveillance awareness levels as well as institutional trustworthiness. The majority of participants belong to the category of young adults together with early-career professionals. Statistical data reveals that 58.1% of the respondents belonged to the 26–32 age category while 17.3% were between 18–25 years old and 15.5%

were in the 33–40 years range with 9.1% belonging to groups above 50 years old. Younger people in this population actively use digital technology so they experience digital surveillance directly while older individuals are less impacted. The active platform usage of respondents allows to study current privacy dynamics and trust issues in contemporary societal structures. The demographic sample effectively presents an ideal research group that allows to explore various digital surveillance effects on public trust across male-female, educational background and age divisions.

Table 1

The results of Reliability Test

Demographic Variable	Category	Frequency (N)	Percentage (%)
Gender	Female	134	60.9
	Male	86	39.1
Education	Undergraduate Degree	108	49
	Graduate Degree	72	32.7
	Postgraduate Degree	40	18.1
Age	18–25 years	38	17.3
	26–32 years	128	58.1
	33–40 years	34	15.5
	Above 50 years	20	9.1

N=220

Table 2 shows that reliability tests indicate substantial internal consistency for all evaluating variables which confirms the robust instruments used in this research project. Digital Surveillance displayed a Cronbach's α of 0.87 across six items (DS1 to DS7) which proves its reliability in recording subject assessments about digital monitoring practices. The reliability of users' privacy-related concerns was validated through Cronbach's α at 0.84 based on five items (PC1 to PC10). The four items of the Regulatory Framework variable (RF1 to RF5) achieved satisfactory reliability when measured by Cronbach's α which was 0.81. The items in the survey display consistent performance for measuring the degree to which people perceive existing privacy laws and data protection rules to be robust and efficient. The Trust in Modern Societies scale with six items (TMS1 to TMS7) demonstrated the highest reliability score of 0.88 which indicates the consistent evaluation of public trust in societal institutions and digital ecosystems. The statistical reliability metrics employed in this research indicate model acceptability because all the scales surpass the commonly recognized threshold of 0.70 to assess the interdependent relationship between digital surveillance and privacy control and regulatory oversight and societal trust.

Table 2

The results of Reliability Test

Measured Variables	Items Range	Cronbach's α Coefficient
Digital Surveillance	DS1 to DS7	0.87
Privacy Concern	PC1 to PC10	0.84
Regulatory Framework	RF1 to RF5	0.81
Trust in Modern Societies	TMS1 to TMS7	0.88

The Confirmatory Factor Analysis results in Table 3 demonstrate robust construct validity and reliability for the research measurement model used in this investigation. The CFA analysis revealed that all measured variables had strong correlations with their related constructs as indicated by standardized factor loadings between 0.64 to 0.91. The factor loadings of Digital Surveillance ranged from 0.68 to 0.88 while Average Variance Extracted reached 0.66 and Composite Reliability reached 0.89 thus verifying both internal

consistency and convergent validity. The measurement scale for Privacy Concern showed superior measurements through its factor loadings between 0.70 and 0.91 and it's AVE of 0.69 and CR of 0.91. These results indicate strong success in measuring individuals' privacy fears and perception. The measurement properties of the Regulatory Framework construct proved robust with loadings between 0.64 and 0.85 and an AVE of 0.63 and a CR of 0.88 indicating satisfactory measurement of perceptions about legal protections and governance structures. The measurement indicators for Trust in Modern Societies reached their peak with factor loadings ranging between 0.72 to 0.90 and produced an AVE of 0.71 and CR of 0.92 making it a reliable construct. Excellent convergent validity and internal consistency emerge from the CFA results since both AVE values meet or exceed 0.50 while CR values reach or exceed 0.70. These findings ensure the structural reliability of the research model.

Table 3

The results of Confirmatory Factor Analysis

Measured Variable	Standardized Factor Loading	Convergent Validity	
		AVE	CR
Digital Surveillance	0.68 – 0.88	0.66	0.89
Privacy Concern	0.70 – 0.91	0.69	0.91
Regulatory Framework	0.64 – 0.85	0.63	0.88
Trust in Modern Societies	0.72 – 0.90	0.71	0.92

The results presented in Table 4 provide insightful evidence regarding the interrelationships among the core constructs of the study Digital Surveillance, Privacy Concern, Regulatory Framework, and Trust in Modern Societies. The diagonal values represent the square roots of the Average Variance Extracted (AVE), all of which exceed their corresponding inter-construct correlations, indicating strong discriminant validity among the variables. Notably, Digital Surveillance is significantly and negatively correlated with Trust in Modern Societies ($r = –0.45$, $p < .01$), confirming that increased surveillance is associated with a decline in public trust—supporting the theoretical premise of this study. Furthermore, Digital Surveillance also shows a significant negative correlation with Privacy Concern ($r = –0.42$, $p < .05$), suggesting that as surveillance increases, individuals' concerns about privacy also intensify. In contrast, Privacy Concern is negatively associated with Trust ($r = –0.35$, $p < .01$), highlighting that greater apprehension about personal data use undermines public confidence in societal institutions. Interestingly, the Regulatory Framework exhibits a positive and significant relationship with Trust ($r = 0.30$, $p < .01$) and a modest yet significant positive correlation with Privacy Concern ($r = 0.28$, $p < .05$), indicating that robust legal safeguards not only mitigate privacy concerns but also enhance societal trust. Overall, these correlation results not only validate the hypothesized pathways in the mediation-moderation model but also affirm the theoretical interconnectedness of digital surveillance dynamics, reinforcing the need for effective regulatory policies to protect privacy and uphold institutional trust in modern digital environments.

Table 4

Pearson correlation and AVE root value

	1	2	3	4
Digital Surveillance	0.81			
Privacy Concern	–0.42*	0.83		
Regulatory Framework	–0.10	0.28*	0.79	
Trust in Modern Societies	–0.45**	–0.35**	0.30**	0.84

The mediation analysis results in Table 5 provide compelling evidence for the indirect effect of privacy concern in the relationship between digital surveillance and trust in modern societies. The path from Digital Surveillance to Privacy Concern (path a) is statistically significant with a coefficient of 0.48 ($p < .001$), indicating that higher levels of surveillance are strongly associated with increased concerns over personal

data privacy. Similarly, the path from Privacy Concern to Trust in Modern Societies (path b) is also significant with a negative coefficient of –0.44 ($p < .001$), suggesting that individuals who experience heightened privacy concerns are less likely to trust societal institutions and systems. Moreover, the direct effect of Digital Surveillance on Trust (path c) remains significant and negative ($B = –0.33$, $p = .001$), illustrating that even without the mediator, surveillance still directly erodes trust. However, the indirect effect ($ab = –0.21$), with a 95% confidence interval that does not include zero (CI = –0.31 to –0.12), confirms that Privacy Concern significantly mediates this relationship. This partial mediation effect suggests that Digital Surveillance undermines trust both directly and indirectly through the intensification of privacy concerns. These findings reinforce the conceptual framework of the study and validate the proposed mediation model. They highlight that individuals' trust in modern societies is not solely shaped by the presence of surveillance technologies but is deeply influenced by the psychological and emotional implications of perceived privacy invasion. The statistical significance and strength of this mediation effect provide strong empirical support for Hypothesis 2, emphasizing the critical role of privacy concerns in shaping public trust in an era of pervasive digital monitoring.

Table 5

Mediation Analysis through Bootstrapping Method

Path	Coefficient (B)	SE	T	P	95% CI (Lower)	95% CI (Upper)
Digital Surveillance → Privacy Concern (**a**)	0.48	0.07	6.86	<.001	0.34	0.62
Digital Surveillance → Trust in Modern Societies (**c**)	–0.33	0.09	–3.67	0.001	–0.52	–0.14
Indirect Effect (ab)	–0.21	0.05			–0.31	–0.12
Privacy Concern → Trust in Modern Societies (**b**)	–0.44	0.08	–5.50	<.001	–0.60	–0.28

The moderation analysis results in Table 6 provide strong evidence for the moderating role of the regulatory framework in the relationship between digital surveillance and trust in modern societies. The direct path from Digital Surveillance to Trust is significantly negative ($B = –0.38$, $p < .001$), indicating that, as surveillance increases, public trust significantly decreases. Conversely, the Regulatory Framework has a positive and significant effect on trust ($B = 0.33$, $p < .001$), suggesting that strong regulatory measures enhance public confidence in institutions and digital environments. Most notably, the interaction term (Digital Surveillance × Regulatory Framework → Trust) is positive and significant ($B = 0.18$, $p = 0.003$), with a confidence interval ranging from 0.06 to 0.30, confirming that the regulatory framework significantly moderates the impact of digital surveillance on trust. The strength of data protection laws together with regulatory safeguards acts to reduce or weaken surveillance's negative impact on trust. The protection of robust regulatory frameworks helps diminish trust deterioration due to tracking methods while non-existent regulations lead to increased trust breakdown. Regulatory oversight plays a fundamental role in shaping public perception because the study results demonstrate its importance in reducing the trust impact of surveillance practices. In order to achieve public trust in the digital era security, entities need to both minimize invasive monitoring practices and demonstrate effective privacy regulations and their implementation procedures to users.

Table 6

Moderation analysis through bootstrapping method

Path	Coefficient (B)	SE	T	P	95% CI (Lower)	95% CI (Upper)
Digital Surveillance → Trust in Modern Societies	–0.38	0.08	–4.75	<.001	–0.54	–0.22
Regulatory Framework → Trust in Modern Societies	0.33	0.07	4.71	<.001	0.19	0.47
Digital Surveillance × Regulatory Framework → Trust in Modern Societies	0.18	0.06	3	0.003	0.06	0.3

DISCUSSION

Through empirical analysis the current research demonstrates how digital surveillance affects public trust when viewed through privacy concerns and affected by regulatory frameworks in modern societies. The study proves its theoretical principles as well as delivers missing information to existing academic literature through confirmed empirical evidence for its combined mediation-moderation framework. The results supported all formulated hypotheses thus showing direct relationships which define digital society reactions to surveillance technology. The research data showed digital surveillance creates negative effects on trust in modern societies with a correlation strength value of –0.45 at $p < .001$ which validated the first Hypothesis. The term "surveillance capitalism" emerged originally from (Zuboff, 2023). When he argued against entities revealing user data through unauthorized data commodification. Extensive surveillance practices weaken public faith while highlighting the lack of user knowledge regarding data utilization (Lyon, 2018). What sets this study apart is its quantification of the effect, offering empirical strength to what had been largely conceptual discourse. Unlike previous studies that relied on qualitative methods or general surveys, this research provides statistically robust evidence of how digital surveillance directly erodes trust. Furthermore, drawing on Communication Privacy Management Theory, this study confirms that the loss of perceived control over personal information disrupts individuals' psychological boundaries, leading to resistance, anxiety, and a weakening of institutional confidence. While earlier literature often emphasized national security justifications (Fuchs, 2019), our findings caution that the benefits of surveillance do not automatically translate into societal acceptance, especially in contexts where the mechanisms of data collection remain opaque. This suggests that unless digital surveillance is accompanied by strong safeguards, its unintended consequence is a breakdown in public trust.

Second Hypothesis was also supported by the data, revealing that privacy concerns significantly mediate the relationship between digital surveillance and trust (indirect effect = –0.21, 95% CI = [–0.31, –0.12]). This finding is consistent with studies by (Smith et al., 2011; Solove, 2021), who emphasized that privacy violations are not merely technical but deeply emotional, affecting individuals' sense of agency and control. When people believe their personal information is vulnerable to misuse, they are less likely to trust the institutions managing these technologies. This mediating effect adds a critical layer to the surveillance-trust dynamic by demonstrating how privacy concerns operate as a psychological filter. The study supports the findings of a study in which researcher argued that the value of privacy is inherently tied to personal freedom, and that the erosion of privacy leads to alienation and social disengagement (Byford, 2017). However, while Westin's work was largely conceptual, the current study offers empirical evidence showing that privacy concern is not only a consequence of surveillance but a powerful determinant of trust.

The research adopts Communication Privacy Management (CPM) Theory created by (Petronio, 2002), through its implementation in institutional surveillance settings. CPM theory normally applies to boundary management of personal information disclosure within interpersonal relationships but this research further extends its use to institutional environments which implement surveillance technology. According to CPM theory individuals possess personal data ownership and establish disclosure rules by trusting others while

considering the risk factors to their privacy. Users do not comply with surveillance systems unless institutions effectively demonstrate data management capabilities and honor their privacy limits. Before the present research, another research developed CPM applications within the domains of online self-disclosure and health communication (Child et al., 2009). The present investigation extends these research limits through its exploration of personal privacy management alongside institutional trust and digital governance enabling deeper understanding about privacy influence on societal acceptance of surveillance systems.

The third hypothesis was validated by the significant interaction between digital surveillance and regulatory framework on trust ($\beta = 0.18$, $p = .003$). This finding confirms that robust regulatory environments can significantly buffer the negative impacts of surveillance, supporting prior research by (Barth & De Jong, 2017; Tikkinen-Piri et al., 2018). When individuals are aware that regulatory safeguards such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) exist, their concerns are mitigated, and institutional trust is more easily maintained. This study thus makes a key contribution by empirically validating the moderating role of regulation. While, previously emphasized the importance of regulatory oversight, most studies stopped short of testing its moderating capacity (Bennett & Raab, 2017). The current research bridges that gap, demonstrating how trust outcomes differ depending on the strength of the regulatory environment. In contrast to studies that have viewed regulation as a background condition, this study treats it as a dynamic variable capable of reshaping public perceptions. It suggests that legal frameworks not only ensure accountability but also serve as psychological assurances that protect the social contract in digital spaces. The positive moderation effect illustrates that individuals are more tolerant of surveillance when they perceive institutions as operating under ethical and enforceable boundaries.

This research successfully addresses the theoretical and empirical gaps outlined in the introduction. Whereas previous studies have treated digital surveillance, privacy concerns, and regulatory mechanisms as isolated variables, this study integrates them into a comprehensive mediation-moderation model. By doing so, it offers a full-spectrum analysis of how digital surveillance is experienced, perceived, and ultimately internalized by society. Prior research (Richards, 1934; Van Dijck, 2014), has called for deeper investigation into the mechanisms driving the public's acceptance or rejection of surveillance. However, few studies have empirically tested how privacy concerns function as a mediator or how regulation acts as a moderator. This study fills that gap by deploying a robust quantitative framework with clear causal pathways, validated through structural equation modeling and bootstrapping techniques. By addressing these limitations, the current research contributes to a growing scholarly discourse on digital ethics, surveillance legitimacy, and public engagement. It emphasizes that trust in modern societies is not just a function of technical efficiency but deeply rooted in perceptions of fairness, transparency, and autonomy.

Theoretical Contribution

The theoretical contribution of this study extends Communication Privacy Management (CPM) Theory to digital surveillance situations to show the relationship between individual perception of personal information privacy and unauthorized monitoring violations that lead to erosion of trust. Empirical evidence through mediation-moderation modeling indicates privacy concerns serve as mediators to the adverse connection between digital surveillance strength and trust formation but regulatory structures lessen this impact on surveillance results. The study analyzes institutional trust at an organizational scale together with human psychological trust reactions to create a thorough understanding of surveillance and privacy perceptions as trust determinants. The study offers scientific evidence which validates the theoretical arguments against surveillance capitalism through its assessment of public trust levels. Rather than existing in isolation the Technology Acceptance Model gains expansion through this study because it shows trust along with privacy and regulatory clarity serve as fundamental factors for public digital system adoption. This research presents a full system which demonstrates how modern societies develop trust through the influence of digital governance along with ethical oversight and personal privacy standards.

Practical Implications

The findings of this study offer several practical implications for policymakers, technology companies, and civil society. The study demonstrates to both governmental entities and regulatory organizations the absolute need to create robust privacy lawful frameworks that enforce their regulations. Laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) serve not only as legal safeguards but also as trust-building mechanisms. Users establish trust through institutional arrangements because protected information exists under both enforceable and transparent regulatory structures. Digital platforms need businesses to perform ethical contractual data operations and establish transparent data management systems when collecting research-oriented information. The combination of privacy-by-design frameworks with open user communication helps organizations achieve better customer trust which leads to prolonged organizational loyalty. Recent studies call for advocacy groups to establish privacy education as their most essential educational initiative. The public develops better awareness about their data rights after receiving enhanced educational programs on digital literacy and data rights therefore decreasing their concern about surveillance. New system development demands system designers and developers to integrate psychological and emotional features into trust framework construction. Users develop favorable sentiments about surveillance systems through technologies which provide them sovereign control of their data and consent processes. Organizations now have an actionable method to bridge technological progress with ethical accountability within the present digital age.

CONCLUSION

The research demonstrates conclusively how digital surveillance strongly reduces public trust formation in contemporary modern societies. Individuals monitor personal data privacy concerns that display mental and emotional attitudes toward observed invasions of their information while revealing this connection through direct analysis. When accompanied by strong regulatory frameworks which act as protective mechanisms trust levels remain less likely to deteriorate. People tend to accept surveillance practices when they notice effective legal safeguards exist protecting their privacy. Surveillance practices create stronger privacy concerns and reduce trust in institutions when regulatory structures remain unclear or nonexistent in a specific environment. The research demonstrates that digital trust base goes beyond system performance since people form trust based on their perceptions about how fair institutions are and their levels of autonomy and accountability. This research delivers an enhanced comprehension about how surveillance shapes the interaction between privacy principles and regulatory frameworks and trust mechanisms which determines the path that digital societies will follow by maintaining proper balance between technological innovations and ethical oversight systems. Research indicates that trust in the digital environment depends on increased privacy-preserving technology development along with transparent policymaking alongside public education initiatives.

LIMITATIONS AND RECOMMENDATIONS

This research delivers new knowledge and has specific boundaries that need clarification. The biased nature of the study subjects presents a significant research obstacle because most of them are young people who hold advanced educational qualifications. The experimental data cannot be directly applied to groups that exclude both senior citizens and unskilled digital users. Forbidding geographical validity in this study because it failed to analyze how regional attributes along with surveillance rules impact community responses to monitoring and trust policies. The main drawback of this research results from its cross-sectional design because it obtains information solely from a single time point. Researcher should conduct future studies through longitudinal analysis to monitor how trust develops when surveillance technologies and policy regimes undergo transformations. The investigated research did not delve into different moderating elements such as political beliefs and media influence and past data security incidents although it evaluated privacy concerns alongside regulatory systems. Future research should focus on these available areas because they offer substantial investigative possibilities. Research conducted through comparative analysis with nations that have different surveillance cultures and laws can enhance the development of the mediation-moderation model. Understandings concerning future digital governance would benefit from

studies about the impact of new surveillance technologies including AI surveillance and facial and biometric data systems on trust levels.

REFERENCES

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

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058.

Bednar, P., & Sadok, M. (2024). Information Security: Still Not my Job! In *Navigating Digital Transformation: Organizational Change, Digital Work, and Individual Behavior* (pp. 63-74). Springer.

Belanger, F., & Carter, L. (2012). Digitizing government interactions with constituents: an historical review of e-government research in information systems. *Journal of the Association for information Systems*, *13*(5), 1.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, *17*(2), 165-176.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017-1041.

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668-2690.

Byford, K. S. (2017). Privacy in cyberspace: Constructing a model of privacy for the electronic communications environment. In *Privacy* (pp. 387-460). Routledge.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, *60*(10), 2079-2094.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors*, *23*(3), 1151.

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.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639-655.

Fano, R. (1968). Privacy and Freedom. In: JSTOR.

Fuchs, C. (2019). *Nationalism on the Internet: Critical theory and ideology in the age of social media and fake news*. Routledge.

Kleynhans, D. J., Heyns, M. M., & Stander, M. W. (2022). Authentic leadership and flourishing: Do trust in the organization and organizational support matter during times of uncertainty? *Frontiers in psychology*, *13*, 955300.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture: Intercultural dynamics of privacy calculus. *Wirtschaftsinformatik*, *54*, 123-133.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Mannan, M. A. (2025). Surveillance and Privacy: Examining the Complex Interplay Between National Security and Individual Freedoms. In *Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions* (pp. 465-486). IGI Global Scientific Publishing.

Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of business ethics*, *160*(4), 835-850.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Neto, E. P. d. A. R. J. (2023). *Paying for privacy in a digital age: willingness to pay for attributes in a VPN (Virtual Private Network) service, and its relation to privacy literacy*

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Richards, N. M. (1934). The Dangers of Surveillance'(2013). *Harvard Law Review*, *126*, 1934.

Rodrigues, S., Correia, R., Gonçalves, R., Branco, F., & Martins, J. (2023). Digital marketing's impact on rural destinations' image, intention to visit, and destination sustainability. *Sustainability*, *15*(3), 2683.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

Solove, D. J. (2010). *Understanding privacy*. Harvard university press.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, *126*, 1880.

Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, *89*, 1.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 2053951717736335.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ*, *13*, 203.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society*, *12*(2), 197-208.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, *26*(3), 135-174.

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and emotion*, *18*(2), 129-166.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203-213). Routledge.