

Privacy in the Digital Age: Are We Being Watched? – Discusses Concerns about Online Surveillance

Naeem Ullah Tariq¹, Khansa Waseem²

¹PhD Scholar, School of Media and Communication, Shanghai Jiao Tong University, Shanghai, China

²Research Scholar, Department of Media and Communication Studies, Rawalpindi Women University, Pakistan

Correspondence: naeemutariq@sjtu.edu.cn¹

ABSTRACT

Aim of the Study: This study aims to investigate the degree of awareness, perception, and satisfaction regarding data privacy, surveillance use, and legal protection in the digital age of social media users in Rawalpindi, Pakistan.

Methods: In employing a quantitative, descriptive survey design. Structured questionnaires a five-point Likert scale was used to collect data from delegates of the sample population who were active social media users. In total, it distributed 270 questionnaires using a non-probability convenience sampling technique, which yielded 253 valid responses (93.7% response rate). SPSS was used for the analysis of data, which outputs means, standard deviations, frequencies, and percentages so that it is possible to confirm the robustness and reliability in the findings.

Results: The Findings shows that about 61.3% of respondents asserted that their activities in at least one of their social media accounts are under watch, while only 45.7 percent expressed satisfaction with what they regard as existing data protection mechanisms set up by their government. A more substantial percentage expressed their lack of satisfaction concerning the adequacy of legal safeguards put into place, such as the PECA Act, concerning the commercial use of the information of individuals without them expressly consenting to that. Furthermore, trust concerning government consumption of data was low and it was perceived by 50% that current laws could infringe the freedom of expression as well.

Conclusion: The study conclude that moderate familiarity exists as to the privacy rights and surveillance dynamics among social media users in Rawalpindi, but intense unease came along with it and the citizenry registered high mistrust toward state or corporate data governance. The findings point clearly to a disconnect between user awareness and institutional accountability. Such multi-faceted approaches for addressing this gap include policies centered on users and efforts toward global legal frameworks against promoting digital transparency to restore trust in digital ecosystems among users.

Keywords: Privacy, Digital Age, Online Surveillance, Online Media Users.

Article History

Received:
February 17, 2026

Revised:
April 21, 2026

Accepted:
April 25, 2026

Online:
April 28, 2026

1. INTRODUCTION

Now, in our digital world, privacy has become almost literally nonexistent (Safdar, 2023; Hassan & Safdar, 2022). Indeed, while most people spend most of their time and activities in communicating, trading, interacting with one another, and being entertained through the internet, they unknowingly open up millions of private matters concerning themselves to companies. Such companies involve myriad private companies, governmental authorities, or other types of conglomerate- private industries and revenue-generating -that collect, store, or analyze user data mostly without explicit consent or even knowledge (Safdar, 2021; Safdar & Abbasi, 2020; Zuboff, 2019; Shabir et al., 2015).

The issue of surveillance and tempers brought the attention of the world by revelations such as those made under debrief of the former NSA contract worker Edward Snowden in 2013 (Greenwald, 2014).. Beyond that growing area into which corporations were increasingly invading citizen privacy and where the government was spying on citizens' digital communications, came another phenomenon- surveillance capitalism as described by Shoshana Zuboff. This concept showed how companies were translating data into dollars through predicting and behaving human manipulation with the help of data analytics (Zuboff, 2019). Indeed, this has posed ethical and legal questions on the digital rights and freedoms of individuals today, together with erosion of privacy when it becomes increasingly normative to say you are "being watched."

Besides raising the aforementioned critical questions of whether privacy can withstand life in data-heavy societies, what should societies do between national security and individual freedoms? And maybe most important of all, do we even know who is watching us- and why?

1.1 Problem Statement

In an era of digitization, online surveillance poses serious concerns with digitization-as-communication, shopping, and entertainment-growing as a major consideration. While convenience and accessibility have become catchwords for these platforms, governments, corporations, and others collect personal data on ethical and privacy grounds. Massive tracking of online user behavior is widely conducted covertly and without user consent. Security, convenience, and individual rights have ignited debates around this issue. This study tackles the issue of the ethics of online surveillance while outlining how data sharing affects personal levels of privacy, autonomy, and trust with digital service providers. It also looks into public consciousness and perception of surveillance practices, pointing to the disconnection between technological advances and people's knowledge of their rights. With the continued advancement of surveillance technologies, understanding the relevant ethical and privacy concerns is critical in educating public discourse on digital rights and informing policy development that safeguards people's information.

1.2 Significance

This research bears significant social responsibility by creating awareness for the scope and consequences of online surveillance. By investigating how personal data is collected, monitored, and used, the research serves to educate the public on the risks that digital platforms pose. Given that many users do not know what data might be being tracked, this research helps fill the gap in knowledge, thereby empowering such people to make informed choices about safeguarding their online privacy. Such raised awareness leads to a privacy-aware society, where more people are inclined to protect their personal information and demand more transparency from tech companies, thus encouraging better digital literacy and responsible behavior on the Internet.

1.3 Study Gap

In past some researches, researchers focused on the psychological effects of online surveillance. There are some factors which have not been addressed in past years, so this study aimed to understand the individuals concerns of their data privacy. People are very apprehensive about online surveillance, yet unsurprisingly, many do not know the extent, purpose, and methods by which data are collected by

websites, apps, and digital platforms. Filling this gap is significant in paving a way for the creation of efficient education and transparency tools for digital users.

2. LITERATURE REVIEW

Andrejevic & Selwyn (2022) the article deals with the co-evolution of privacy and surveillance in digital societies: "Surveillance cannot be mentioned among technical issues alone; it's actually a disruption of society, shaping behavior and government". The authors then draw on theory and current cases to show how users act in surveillance environments while data-extraction normalizes it within institutions. The work describes the compelling design of dynamic, policy-based responses to fast-moving, frighteningly changing surveillance ecosystems.

Cooke (2015) a wide-ranging coverage of the digital privacy matters, with a major focus on the ethics embroiled in data collection. Hence, the research will analyze the rift that appears on the individual rights against technological advancement and the delaying legal framework in keeping pace with innovation. Through case illustrations, Cooke would showcase how corporations wield that data power for profit at the users' detriment and perhaps unawares. The article calls for heightened regulatory interventions and public consciousness.

William et al. (2018) this preprint studies the IoT "privacy paradox", where "people are concerned about privacy but will use these intruding technologies anyway". Technical and socio-political factors around privacy in the IoT space and the social aspects of the same. Different models of theory-testing causation have been discussed. Explorative analysis and individual interviews understand the entire potential of getting this up.

Darmody & Zwick (2020) the authors deem to look at digital technologies from a critical perspective examining the tensions surrounding consumer privacy against a backdrop of data-driven capitalism. In so doing, they elaborate on how platforms use the opacity of algorithms to collect and monetize personal data while redefining users as mere sources of behavioral surplus. Among the review's highlights are resistance movements that have recently emerged, such as data activism. However, these schemes operate in a power landscape that undermines the likelihood of individual agency and informed consent.

Clarke (1988) Clarke's trailblazing work describes the concept of "dataveillance," distinguishing it from traditional surveillance. The introduction of computer systems that help to monitor entire populations with aggregations of data was described by him. This was an early study predicting the decline of privacy standards in a digitalized world and criticizing the ethical and policy concerns for democracies of tracking people's data unethically. Clarke puts in place some rudimentary but stringent requirements for the exercise of the concept "dataveillance" and other forms of technological intrusion on civil rights: a focus on the privacy-by-design and accountability of institutions to the people it serves.

Turow (2021) provides an easy read but knowledgeable introduction to the phenomenon of surveillance culture in today's digital society. He discusses a surveillance ecosystem where advertising, data brokers, and social media platforms prop up profiling and targeting practices. This review brings a fruitful connection between academic research and public awareness, thus urging increased digital literacy and stronger data protection laws to empower individuals.

Nissenbaum (2009) created the theory of contextual integrity which states that privacy is best understood in terms of the appropriate flow of information in given contexts. Instead of presenting a simplified argument for privacy as secrecy, she discusses norms and expectations in the sharing of information. This has amounted to a considerable body of work in the science of privacy, offering no small amount of analytical power for the evaluation of surveillance regimes.

Lyon (2007) in a comprehensive overview of surveillance studies, Lyon maps out theoretical frameworks, historical development, and growth in forms of digital monitoring. He sets into view the differentiation of security measures extending beyond consumer profiling to social sorting. The review

emphasizes the logic of embedding surveillance in the very institutions and technologies of our modern times, calling for interjection from various disciplines to contribute toward understandings of privacy rights and public policy.

Gandy (1993) in Gandy's view, the panoptic sort critiques the commodification of personal data. Surveillance technologies classify individuals in a systematic manner—one that strengthens inequalities socially and in terms of control. Drawing from political economy and communication theory, Gandy asserts that race, class, and power intersect in data profiling, thereby providing a critical approach for evaluating surveillance under contemporary purposes.

Zureik & Salter (2005) this edited volume illustrates the global dimensions of surveillance, particularly in relation to the challenges of security, migration, and identity. The contributors analyzed that how surveillance technologies extend state power across the control lines, often under the control of national security. This highlights ethical and legal tensions in biometric tracking, border control, and international data sharing.

Stuart et al. (2019) in their exploration of the psychological aspects of digital privacy, Stuart et al. (2019) focus on how people perceive their privacy/respect for their personal information and its management on the Internet. The authors argue that concerns for privacy are shaped by cognitive biases, social norms, and contextual elements. A description of the "illusion of privacy" is presented, whereby users feel their data are somehow secure, despite overt or covert evidence of massive surveillance. The emotional factors related to privacy violation are further examined, pointing out that anxiety and distrust arise when individuals feel their private information is being exposed. This argument also attributes to social media platforms the role of normalizing data collection and, as a consequence, diminishing users' sensitivity to privacy threats. Digital literacy and transparency can empower users to make informed choices for their privacy, considering the authors. The overall conclusion is that psychological insights should be thought through in the design of policies and technologies that claim to protect privacy while bearing in mind the way humans actually behave and their cognitive limitations.

Wang & Baker (2022) examines the legal ramifications of digital surveillance and what it means today to have a "reasonable expectation of privacy." It specifies that these new surveillance technologies: facial recognition, geolocation tracking, artificial intelligence data mining, etc., have subverted traditional notions of privacy. They analyze legal precedents in the United States and in Europe, with a focus on the tension between national security interests and individual privacy rights. The work critiques the role of technology companies in facilitating mass surveillance, which often skirt privacy laws using vague terms of service agreements. The authors then assess cases where courts decided digital privacy issues and emphasize the inconsistency in legal interpretation. They propose reforms redefining privacy rights in the digital age, ensuring tighter regulation of data collection and more precise legal standards for digital monitoring. The paper concludes by saying that in the absence of serious legal protection, individuals will continue to be subjected to intrusive and often illegal surveillance practices.

Reis et al. (2024) in this research, they analyze the global landscape for privacy laws and how, in each country, the regulation of digital surveillance and data protection differs. The study further considers a few major privacy regulations, namely the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL). The authors identify some key enforcement challenges that arise, such as corporate non-compliance, jurisdictional clashes, and the limited deterrent effect of fines. They argue that privacy laws are often unable to keep pace with rapid advancements in technology and hence, loopholes are left open that allow continued mass surveillance. The article evaluates how various governments weigh security concerns against civil liberties.

Bashir (2021) it is an interesting examination of the changing mechanisms of surveillances in the modern age through the lens of panopticism. The study seeks to reread the classical theories of Bentham and Foucault within the context of contemporary digital surveillance practices. According to Bashir, one of

the distinct transformations of surveillance in modernity from that of the former has been from physical observation to networked surveillance systems, making it mostly technologically dependent. This transformation has altered power dynamics leading to new kinds of control and perhaps exploitation. It will be beneficial to understand how these shifts occur so that they can be addressed in dealing with the intangible risks and complexities that accompany digital surveillance.

Ali et al. (2018) analyze the privacy and security challenges involved with Online Social Networks (OSNs). The authors first mention some threats that arise such as identity theft, unauthorized data mining, and surveillance by bad actors. The architecture of OSNs, which is usually based on very broad sharing and deprivation of user access, mostly results in these threats. This review argues in favor of adding security measures and privacy-gained technologies to protect users. The authors also talk about how user awareness and education can help curb privacy risks that usually come with OSNs.

Manokha (2018) Foucault's Panopticism in the Prisons of Time is applied to the new world of surveillance technology today. It helps explain how technologies that watch everywhere make it imperative for self-discipline in private lives, acting public opinion at every opportunity.

2.1 Theoretical Framework

The study herein uses the lens of the Privacy Paradox theory that grapples with the contradiction between stated concerns about digital privacy and actual digital behavior. The Privacy Paradox was first described by Daniel Solove and subsequently developed by media and communication researchers. The essence of this theory is that users express awareness of the risks of online surveillance and data collection while knowingly offering personal information through digital platforms with little resistance. In the context of the research topic, Privacy in the Digital Age: Are We Being Watched?, it proves to be an interesting starting point for analyzing public opinions on surveillance and data privacy. With an in-depth integration of digital technologies into daily life, the individual finds himself/herself navigating the trade-offs between ease of use and control over personal information. When asked about government surveillance, corporate data mining, or cybersecurity threats, a survey respondent may in fact profess to some discomfort; however, his/her pattern of behavior completely contradicts such expressed discomfort when they engage with smart devices, social media, and cloud-based services.

The explanation of this paradox has many answers, be it illiteracy in terms of the digital world, a feeling of resignation toward ever-present data tracking, or opaque data practices on the part of governments.

Figure 1: Study Model

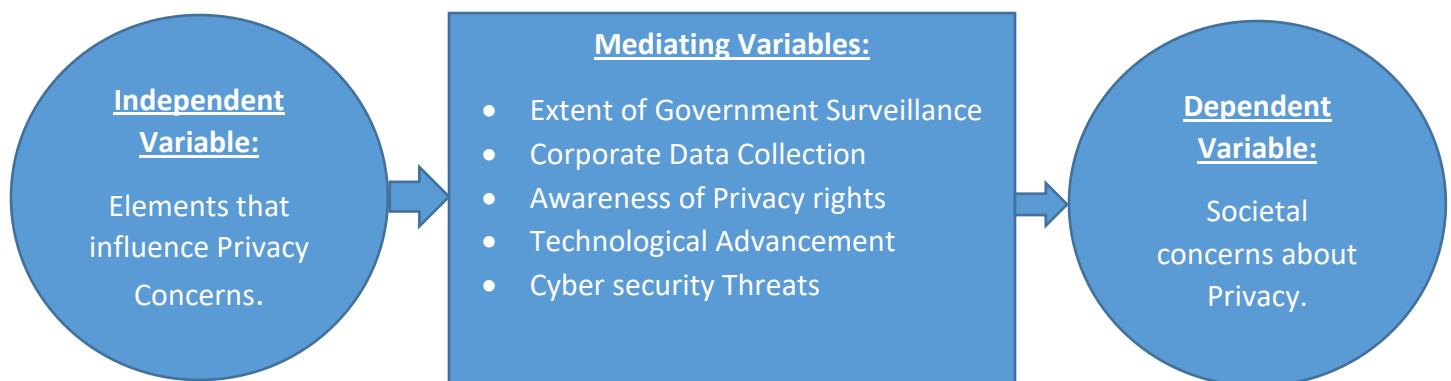


Figure 1 shows that study model consisting of independent variable and dependent variable.

2.2 Hypotheses

- H1: Perceived online surveillance is significantly associated with individuals' privacy concerns.
H2: Perceived online surveillance is positively related to personal data security concerns.
H3: Perceived online surveillance has a significant positive relationship with privacy awareness.
H4: Perceived online surveillance is significantly associated with trust in digital platforms.
H5: Perceived online surveillance is positively associated with protective privacy behaviour.

3. METHODOLOGY

3.1 Research Design

The quantitative research method has been used in this case study to explore privacy concerns about online surveillance in the digital age. The descriptive Statistic research design is followed for online surveys. Likert scale method has been used to collect data and measured results conveniently.

3.2 Population

The population of research study was general public of Rawalpindi, Pakistan who uses social media, so they had shared their concerns about online surveillance in digital age in better way.

3.3 Sample Size and Techniques

The total sample size of the study included (n=253) respondents who completed responses were received. The study applied the most common sample selection; convenience sampling that ensured the selection of respondents meeting the availability and willingness to participate criteria. Though a non-probability sampling method, it is well suited to the study focus, which examines the privacy concerns of the digital age, particularly online surveillance. Consequently, the findings regarded as credible from this high response rate and the convenience sampling technique.

3.4 Data Collection Tool

The well-defined questionnaire and Google form was used to collect data and required demographic information. Questions were made by Dependent and Independent variables by using Likert style method with options Strongly disagree, Disagree, Neutral, Agree and Strongly Agree.

Table 1: *Reliability of the variables*

Construct	No. of Items	Cronbach's Alpha (α)	Reliability Level
Perceived Online Surveillance	8	0.891	Excellent
Privacy Concern	6	0.873	Good
Personal Data Security Concern	6	0.884	Good
Privacy Awareness	6	0.857	Good
Trust in Digital Platforms	6	0.901	Excellent
Protective Privacy Behaviour	6	0.918	Excellent

The reliability analysis presented in table 1 demonstrates that all study constructs exhibit satisfactory to excellent internal consistency. Cronbach's alpha values ranged from 0.857 to 0.918, exceeding the recommended threshold of 0.70, thereby confirming the reliability of the measurement instrument. Protective Privacy Behaviour showed the highest reliability ($\alpha = 0.918$), followed by Trust in Digital Platforms ($\alpha = 0.901$) and Perceived Online Surveillance ($\alpha = 0.891$), indicating excellent reliability. The remaining constructs Privacy Concern ($\alpha = 0.873$), Personal Data Security Concern ($\alpha = 0.884$), and Privacy Awareness ($\alpha = 0.857$)—also demonstrated good internal consistency. These findings confirm that the measurement scales are reliable and appropriate for subsequent inferential statistical analyses.

3.5 Data Analysis Techniques

The data collected for this research was analyzed in SPSS, protecting the reliability and validity of the results. SPSS was responsible for producing statistical outputs such as frequencies, means, standard deviations (SD), and percentages, which were reliable, verifiable, and robust in evidencing the research objectives and conclusion.

4. RESULTS

Table 2: Demographic Information

Sr.	Demographics	Options	<i>f</i>	%
1	Gender	Male	106	41.7
		Female	146	57.5
2	Age	18-27	96	37.8
		28-37	79	31.1
		38-47	57	22.4
		48-57	18	7.1
		Matriculation level/O-level	25	9.8
3	Education Level	Intermediate/A-level	81	31.9
		Bachelor Degree (Graduate)	89	35.0
		Masters	41	16.1
		Above Master	17	6.7
		Unemployed	86	33.9
4	Employment Status	Self-Employed	55	21.7
		Government Employee	48	18.9
		Private Sector Employee	46	18.1
		Freelancer	16	6.3
		Retired	1	0.4
5	Social media usage experience	1-5 years	61	24.0
		6-10 years	123	48.4
		More than 10 years	67	26.4
6	Routine of Social Media daily use	1-2 hours	54	21.3
		3-4 hours	126	49.6
		More than 4 hours	73	28.7
		X (former Twitter)	13	5.1
		Instagram	87	34.3
7	Mostly used application	YouTube	79	31.1
		TikTok	53	20.9
		Facebook	14	5.5
		Others	7	2.8

Table 2 shows that demographic profile of the respondents sheds much light into the composition of the sample as well as social media usage patterns among them. Thus, the participants comprised more females (57.5%) than males (41.7%). In terms of age distribution, a vast majority of the respondents (68.9%) are aged between 18 and 37 years, indicating that the majority are young adults. Educationally, about a third of the population had a bachelor's (35.0%) or master's degree and above (22.8%), justifying a fairly high educational attainment among the respondents. Of all, though 33.9% were unemployed, others were in different situations; some were self-employed (21.7%), in government jobs (18.9%), in private-sector employment (18.1%), and the rest were freelancers (6.3%). The most interesting thing is that most respondents used social media for more than five years (74.8%). This fact widely indicates increased experience using online platforms. It was also very high daily, with almost 78.3% of users reporting spending three hours or more per day using social media. Among different aspects of the study,

when they tried revealing the preference order of platforms, they realized that Instagram tops the list with 34.3 percent, followed by YouTube (31.1 percent) and TikTok (20.9 percent). This is consistent with global trends for today's youth regarding being connected electronically. In summary, these trends articulate the role of social media in the daily lives of these respondents and strongly support further inquiry into its effects on behavioral and psychological outcomes.

Table 3: *Descriptive statistics*

Variables	No. of Items	Mean	SD	MIN	MAX
Perceived Online Surveillance	8	2.419	0.489	1.00	4.00
Privacy Concern	6	2.503	0.563	1.00	4.00
Personal Data Security Concern	6	2.316	0.584	1.00	4.00
Privacy Awareness	6	2.430	0.618	1.00	4.00
Trust in Digital Platforms	6	2.336	0.588	1.00	4.00
Protective Privacy Behaviour	6	2.346	0.608	1.00	4.00

Table 3 presents the descriptive statistics for the six study variables related to privacy in the digital age. The mean scores ranged from 2.316 to 2.503, indicating moderate perceptions across all constructs. Privacy Concern recorded the highest mean score ($M = 2.503$, $SD = 0.563$), suggesting that respondents expressed comparatively greater concern regarding the protection of their personal information. In contrast, Personal Data Security Concern exhibited the lowest mean ($M = 2.316$, $SD = 0.584$). The standard deviations ranged from 0.489 to 0.618, reflecting relatively low to moderate variability in participants' responses and indicating a reasonable level of consistency across the sample. Overall, the descriptive statistics suggest that respondents demonstrated moderate levels of perceived online surveillance, privacy awareness, trust in digital platforms, and protective privacy behaviours, providing an appropriate basis for subsequent inferential analyses.

Table 4: *Correlations among variables*

Variables	Mean	SD	1	2	3	4	5	6
Perceived Online Surveillance	2.419	0.489	1					
Privacy Concern	2.503	0.563	.411**	1				
Personal Data Security Concern	2.316	0.584	.463**	.582**	1			
Privacy Awareness	2.430	0.618	.328**	.471**	.519**	1		
Trust in Digital Platforms	2.336	0.588	.461**	.546**	.613**	.487**	1	
Protective Privacy Behaviour	2.346	0.608	.437**	.564**	.591**	.521**	.598**	1

Notes. Pearson correlation coefficients are reported. N = 253 (listwise deletion). ** Correlation is significant at the 0.01 level (2-tailed) ($p < .001$).

Table 4 presents the two-tailed Pearson correlation coefficients among the six study variables. The results indicate that all correlations are positive and statistically significant ($p < .001$), suggesting meaningful associations among perceptions of online surveillance and the five privacy-related constructs. Perceived Online Surveillance exhibited moderate positive correlations with Privacy Concern ($r = .411$), Personal Data Security Concern ($r = .463$), Privacy Awareness ($r = .328$), Trust in Digital Platforms ($r = .461$), and Protective Privacy Behaviour ($r = .437$). Inter-correlations among the dependent variables ranged from .471 to .613, indicating moderate relationships while remaining below the commonly accepted multicollinearity threshold of 0.80. These findings suggest satisfactory discriminant validity among the constructs and provide preliminary support for the proposed conceptual framework investigating privacy perceptions in the digital age.

Table 5: Overall hypotheses results

Hypothesis	Relationship	r	p	Decision
H1	Online Surveillance → Privacy Concern	0.411	< .001	Supported
H2	Online Surveillance → Personal Data Security Concern	0.463	< .001	Supported
H3	Online Surveillance → Privacy Awareness	0.328	< .001	Supported
H4	Online Surveillance → Trust in Digital Platforms	0.461	< .001	Supported
H5	Online Surveillance → Protective Privacy Behaviour	0.437	< .001	Supported

Overall in table 5, the analyses indicate that perceived online surveillance is significantly and positively associated with all five privacy-related outcomes ($p < .001$). The strongest relationships were observed with personal data security concern ($r = 0.463$) and trust in digital platforms ($r = 0.461$), while the weakest, though still meaningful, association was found with privacy awareness ($r = 0.328$). These findings collectively support the argument that increased perceptions of online monitoring influence individuals' concerns, awareness, trust, and protective behaviours regarding digital privacy.

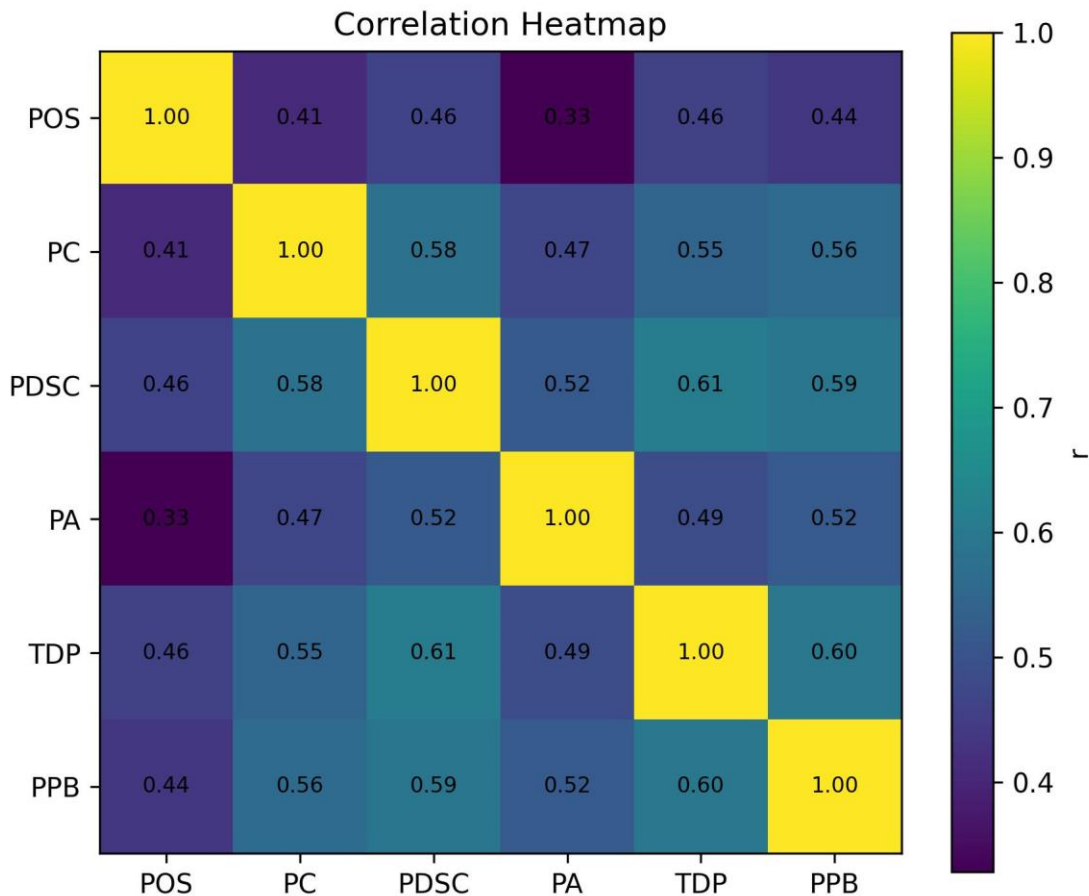
Figure 2: Heatmap of the correlations

Figure 2 Pearson Correlation Heatmap of Study Variables. The heatmap illustrates the two-tailed Pearson correlation coefficients among the six study variables related to privacy in the digital age. All relationships are positive and statistically significant ($p < .001$), indicating that higher perceptions of online surveillance are associated with greater privacy concern, stronger personal data security concern, increased privacy awareness, higher trust-related evaluations of digital platforms, and more protective privacy behaviours. The strongest correlation was observed between Personal Data Security Concern and

Trust in Digital Platforms ($r = .613$), whereas the weakest, yet still significant, relationship was found between Perceived Online Surveillance and Privacy Awareness ($r = .328$). Overall, the heatmap demonstrates moderate to moderately strong associations among the study constructs, supporting the proposed conceptual framework while indicating no evidence of problematic multicollinearity (all $r < .80$).

5. DISCUSSION

The findings of this study correlate with the wider literature depicting an awakening public opinion about digital surveillance and the erosion of online privacy. Most participants experienced online surveillance (61.3% and 63.0%), corroborating Andrejevic and Selwyn's (2022) view that surveillance and privacy are contending upon twin disruptions continuously shaping the vision of the public in the digital era. That satisfaction rates with privacy protection measures fell at 45.7% and with cyberthreats controls at 49.6% lends further credence to Cooke's (2015) assertion that these protective measures have failed to keep pace with technological advancements and instill a sense of security in users. In a similar manner, these users observing mechanisms for online fraud prevention as ambiguous or ineffective (58.3%) also appear to support Darmody and Zwick's (2020) assertion that the surveillance economy thrives in opacity, leaving its users uncertain as to where and for what purpose their data is being co-opted. Average awareness of government surveillance stands at a low score ($M = 2.38$, $SD = 0.890$), whereas concern over government monitoring infringing on privacy is justifiably higher ($M = 2.56$, $SD = 0.943$), replicating the findings of Turow (2021) on the low public trust in state affiliations with surveillance data. There is low trust in government surveillance, with only 50% supporting legal frameworks such as the PECA Act, and a mean of 2.78 indicating that respondents were skeptical. Lyon's (2007) analysis that modern surveillance goes beyond national security into ordinary social life has ethical and democratic implications. Further support by respondents for requiring corporate consent ahead of data collection ($M = 2.22$) and the profit-oriented use of that data ($M = 2.12$) on the other hand help reinforce Zuboff's (2019) idea of surveillance capitalism, which treats user data as a commodity that technology corporations extract from the users and sell, often without explicit knowledge or consent from the users. Nissenbaum's (2009) framework of "contextual integrity" finds validation here as well. The respondents' conflicting perspectives on legal frameworks and privacy rights seem to imply that normative expectations and actual data-handling practices do not match. A general belief that some shields exist (47.2%) but are either poorly enforced or simply out of reach would seem to corroborate Clarke's (1988) early reflections to the effect that and "dataveillance" estranged due to institutional neglect and technical complexity.

6. CONCLUSION

The study concuded that the digitally literate masses are aware of forms of surveillance in the online sphere but remain quite uneasy as well as suspicious of the measures put in place to secure their privacy. The participants have a fairly moderate understanding of governmental and corporate surveillance; however, this has been hogged with an equal measure of disbelief in the effectiveness of existing legal and technological protections. This difference between users' understanding of data privacy issues and their confidence in enforcement mechanisms denotes a longstanding "privacy paradox"- namely, worrying was not translated into evident control or actual management of personal information. In addition, the most important discontent with existing policy systems and institutional safety bogged much more profound social thought about losing digital self-sovereignty. The ambivalence toward laws like this PECA Act along with all the worry surrounding monetization of data by corporations and state surveillance only insists on problems that demand extensive, clear, and, indeed ethically guided data governance policies. While these gaps require stronger legal protections, they also involve architectural frameworks that would serve user-centric digital modeling placing personal agency, informed consent, and fair data stewards at the center of such architecture.

Acknowledgements

None.

Conflict of Interest

Authors declared NO conflict of interest.

Funding Source

The authors received NO funding to conduct this study.

ORCID iDs

Naeem Ullah Tariq ¹  <https://orcid.org/0009-0002-7713-3971>

Khansa Waseem ²  <https://orcid.org/0009-0007-2770-9684>

REFERENCES

- Ali, S., Islam, N., Rauf, A., Ud Din, I., Guizani, M., & Rodrigues, J. J. P. C. (2018). Privacy and security issues in online social networks. *Future Internet*, 10(12), 114. <https://doi.org/10.3390/fi10120114>
- Andrejevic, M., & Selwyn, N. (2022). Surveillance and privacy as coevolving disruptions. *Journal of Digital Social Research*, 4(2), 1–19. <https://doi.org/10.1080/25741292.2022.2086667>
- Bashir, M. (2021). Surveillance and panopticism in the digital age. *Qlantic Journal of Social Sciences and Humanities*, 2(1), 11–16. <https://doi.org/10.55737/qjssh.779670819>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512. <https://doi.org/10.1145/42411.42413>
- Cooke, L. (2015). Privacy in the digital age. *Journal of Information Ethics*, 24(1), 54–65. <https://doi.org/10.3172/JIE.24.1.54>
- Darmody, A., & Zwick, D. (2020). Digital technologies: Tensions in privacy and data. *Journal of Consumer Research*, 47(5), 873–892. <https://doi.org/10.1093/jcr/ucaa045>
- Gandy, O. H. J. (1993). *The panoptic sort: A political economy of personal information*. Westview Press.
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
- Hassan, S.A.U., Safdar, G. (2022). Relationship between Self-Esteem and Problematic Use of Facebook among University Students. *Annals of Social Sciences and Perspective*, 3(1), 199–217. <https://doi.org/10.52700/assap.v3i1.83>
- Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.
- Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, 16(2), 219–237. <https://doi.org/10.24908/ss.v16i2.8346>
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: A global review of legislation and enforcement. *International*

- Journal of Applied Research in Social Sciences*, 6(1), 73-88. <https://doi.org/10.51594/ijarss.v6i1.733>
- Safdar G. (2023). Digital Challenges: Unraveling the Connection of Cyberbullying and Students' Social Anxiety. *Online Media and Society*, 4(3), 75-85. <https://doi.org/10.71016/oms/ttjxqc24>
- Safdar, G. (2021). Formation of Global Village: Evolution of Digital Media-A Historical Perspective. *THE PROGRESS: A Journal of Multidisciplinary Studies*, 2, 17-26. <https://doi.org/10.71016/tp/gneph711>
- Safdar, G., Abbasi, A. (2020). Evaluation and Development of Social Media: A Historical Perspective. *Online Media & Society*, 1, 35-44. <https://doi.org/10.71016/oms/343axf25>
- Shabir, G., Safdar, G., Jamil, T., Bano, S. (2015). Mass Media, Communication and Globalization with the perspective of 21st century. *New Media and Mass Communication*, 34, 11-15.
- Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass*, 13(11), e12507. <https://doi.org/10.1111/spc3.12507>
- Turow, J. (2021). Surveillance and privacy in the digital age: A primer for public understanding. *ScholarWorks@Arcadia*. https://scholarworks.arcadia.edu/grad_etd/4/
- Wang, X., & Baker, D. J. (2022). Criminalising privacy in the digital age: The reasonable expectation of not being digitally monitored. *The Journal of Criminal Law*, 86(5), 351-368. <https://doi.org/10.1177/00220183211033150>
- Williams, M., Nurse, J. R. C., & Creese, S. (2018). The perfect storm: The privacy paradox and the Internet-of-Things. *11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 644-652. <https://doi.org/10.1109/ARES.2016.25>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
- Zuboff, S. (2019). Twenty years of surveillance marketing. *Wired*. <https://www.wired.com/beyond-the-beyond/2018/11/twenty-years-surveillance-marketing/>
- Zureik, E., & Salter, L. (2005). *Global surveillance and policing: Borders, security, identity*. Willan Publishing.