Internet Surveillance and the Role of Social Media Companies

Nishant Raj Sarraf

Abstract

Social media platforms collect and analyze large amounts of user data. This enables pervasive surveillance that shapes attention, advertising, and civic life. This paper asks: How do individuals perceive social media surveillance? How do those perceptions relate to privacy behaviors and demographic factors? Building on existing literature about targeted advertising, platform design, and privacy harms, the study combines a technical review of social media infrastructure with an empirical survey. The survey used Google Forms, with 127 responses from August to September 2023. Survey measures were ordinal-coded and analyzed with pairwise exclusion for missing data. Results show 72.4% of respondents believe their activity is monitored. Half (50.4%) are “partially worried” about data being sold. About 68.5% have either deleted platforms or are considering doing so (27.6% deleted; 40.9% considering). Statistical tests indicate a significant association between gender and worry level ($\chi^2(8) = 21.091$, $p = .007$, $V = .228$). The relationship between worry and deleting a platform approached significance ($\chi^2(12) = 19.027$, $p = .088$, $V = .137$). Age was not significantly associated with worry. These findings challenge generational privacy indifference and support targeted interventions for gender-specific concerns.

Introduction: Overview of Social Media Surveillance

Social media apps have transformed how people form relationships, consume news, and construct their identities. This connectivity depends on systems that collect and analyze large amounts of behavioral and social data. Platforms focus on capturing attention and enabling targeted advertising. These commercial logics drive surveillance practices that shape political persuasion and civic life [1][2]. Companies also share data with or respond to requests from state actors. This extends surveillance into governance and law enforcement [3]. Scholars describe social media surveillance through distinct practices: collaborative identity construction, monitoring of social ties, searchable social relations, shifting interfaces, and combining diverse social contexts into single profiles [4]. To understand how these elements contribute to surveillance, we can utilize the framework of contextual integrity. This highlights the importance of context and the proper movement of information in privacy. This framework illustrates how platform design fosters surveillance by disrupting contextual norms for information flow.

This paper examines how users perceive social media surveillance and how these perceptions relate to privacy behaviors and demographic factors. The study combines a brief technical review of platform mechanisms with an anonymous survey. The survey was administered via Google Forms using snowball sampling (N = 127, August–September 2023). Survey items were ordinal-coded and analyzed with pairwise exclusion and chi-square tests.

Key findings are concise. Most respondents (72.4%) believed they were monitored on platforms. Concern about companies selling information was moderate. In total, 50.4 percent reported partial worry, 22.0 percent expressed worry, and 7.9 percent expressed extreme concern. Protective intentions were common. About 68.5 percent had either deleted platforms or were considering it (27.6 percent deleted; 40.9 percent considering). Statistical tests show a

significant association between gender and worry ($\chi^2(8, N = 127) = 21.091$, $p = .007$, $V = .228$). The relationship between worry and deletion intention approached significance ($\chi^2(12, N = 127) = 19.027$, $p = .088$, $V = .137$). Age was not associated with worry in this predominantly young sample.

These results are significant because they quantify how surveillance perception turns into protective action. They also show how concern varies across groups. Policymakers benefit from understanding which populations report worry and who takes action, as this informs privacy rules. Platform designers should consider how product design and business models raise user concern and may prompt users to leave. Researchers and advocates gain empirical evidence to challenge simplistic claims about generational indifference and to target interventions addressing gendered concerns.

To connect the survey findings to their practical implications, it is essential to examine how one of the primary outcomes of social media surveillance, personalized advertising, shapes user experiences and concerns.

Personalized Advertising

Personalized advertising means tailoring advertisements and content to individuals based on preferences, behaviors, and demographics. Platforms and advertisers combine interaction data (clicks, page views, and search queries), profile attributes, and device or location signals. This helps deliver messages that feel more relevant to each recipient. For example, someone viewing several running shoe product pages may see an ad for the same model. The ad might feature a limited-time discount and a direct retailer link. However, it is essential to approach personalization ethically and transparently. Users must be fully informed and able to consent to their data use. Could there be consent mechanisms that give users real choices about personalization? Providing users with clear options and control is crucial to maintaining trust and following relevant regulations.

Advantages of Personalization in Marketing

Enhanced engagement: Personalized advertising shows more relevant content to the audience. This increases the likelihood users will interact with the brand. Insider Intelligence research found that customized marketing raised engagement for 56% of respondents. Higher engagement is also more likely to benefit both brands and users [5].

Increase leads and conversions: Personalized content matches messaging with interests and past behavior. This increases engagement and conversion chances (such as purchases or newsletter sign-ups). It also offers a better return on investment compared to traditional ads [6].

Improved customer loyalty: Customized marketing increases consumer loyalty [7]. Personalizing messages makes consumers feel recognized and valued, which helps them develop brand loyalty.

Strategies of Personalized Advertising

1. User Data Collection

Social media platforms collect large amounts of data. This includes demographics like age, gender, and location, as well as interests and behaviors (such as liking, sharing, and commenting), browsing history, and more. This data is vital for personalization.

A study by pCloud found that Instagram collects and shares much of its users' data with outside parties, including advertisers. Instagram shares 79% of collected data with third parties, such as contacts, current location, browsing history, and financial data from in-app purchases. Facebook follows, sharing 57% of its collected data with outsiders [8]. The company was among the first to use facial recognition [9], but it has now withdrawn this tool due to abuse and privacy concerns.

Social media data analysis involves collecting raw data and evaluating it against organizational goals. While raw data is valuable, interpretation and persuasion metrics make the most impact [10]. A key question is: who controls these integrated datasets? This power balance often marginalizes users. Analysis is mainly driven by corporate interests, which may not fit user needs. For example, many CFOs may not understand how increased impressions or engagement affect business outcomes. Integrating social data with other sources and aligning it with business goals can enhance strategies. By linking social campaign metrics to web analytics and CRM data, analysts can show concrete business impact. For instance, Campaign A generated 10,000 impressions, a 2% click-through rate (200 clicks), a 5% conversion rate from those clicks (10 purchases), and an average order value (AOV) of $120, yielding $1,200 in revenue. Campaign B, targeted to a high-intent segment, had 5,000 impressions, a 4% CTR (200 clicks), a 10% conversion rate (20 purchases), and an AOV of $150, resulting in $3,000 in revenue. Comparing the data shows that shifting the budget toward the high-intent segment would add $1,800 in monthly revenue (3,000 − 1,200), justifying the budget shift to leadership.

2. Segmentation

Advertisers use collected data to segment users into different groups based on common characteristics. These segments could be broad, such as age groups, or more specific, such as users interested in outdoor sports [11].

Social media audience segmentation represents a significant advancement for brands seeking to move beyond basic demographics and gain a deeper understanding of consumer needs. By leveraging social media data, brands can collect information, organize it into segments, and derive marketing insights that support market growth. Data-driven marketing provides substantial benefits for both brands and their audiences.

In the context of social media surveillance and personalized advertising, audience segmentation refers to the process by which platforms and advertisers categorize individuals into groups based on shared characteristics or behaviors. This segmentation is central to how targeted content is delivered and how surveillance operates at scale.

For this research, audience segmentation is examined as a mechanism that enables personalized advertising and targeted content delivery. Rather than providing practical advice, the focus here is on how segmentation contributes to surveillance practices and influences user experience on social media platforms.

Brands and businesses benefit from targeting platforms where their clients are most active. Utilizing the demographic characteristics of each platform enables brands to tailor their strategies to specific audiences. For example, TikTok attracts a younger demographic [12],

LinkedIn is oriented toward career-related content, and Pinterest has a higher proportion of female users [13]. An effective strategy involves selecting the most appropriate channel for each segment based on platform characteristics and historical performance.

To refine targeting, brands should employ audience filtering techniques. For example, Facebook enables posts to be directed to users based on location. More advanced options are available through sponsored advertising, allowing greater precision in targeting specific audience segments.

Examples:

- Spotify, a music streaming service, utilizes customer segmentation to enhance the user experience. They divide their user base into groups based on location, listening history, and musical interests. This allows Spotify to (a) assemble personalized playlists and listening queues — such as Daily Mix playlists that blend a user's most-listened tracks with similar songs and Discover Weekly lists that surface new artists discovered via collaborative filtering; (b) recommend specific artists, albums, or singles with short rationales (e.g., 'Because you liked X and Y'); and (c) target notifications, in-app banners, and email promotions about nearby concerts, ticket presales, or local album releases to users whose location, listening patterns, and time-of-day habits indicate high purchase or attendance likelihood [14].
- Airbnb is a platform for vacation rentals that utilizes consumer segmentation to tailor marketing campaigns to different traveler demographics. Based on consumer travel interests, such as luxury, adventure, or family-friendly vacations, they segment their audience and develop tailored advertisements that highlight particular locations and lodgings that appeal to each demographic.
- Nike is a sportswear company that creates personalized product recommendations and promotions by utilizing consumer segmentation. Using factors such as activity level, gender, and location, they segment their audience.

3. Dynamic Ad Content

Personalization involves creating ads with dynamic content that changes based on user attributes. For instance, an ad might display different products or offers to users based on their past purchases or browsing history. Dynamic Search Ads utilize content from your website's landing pages to target ads to relevant searches. They can choose from a variety of targeting options to specify which landing pages Dynamic Search Ads should use. One can target groups of URLs using targeting types such as "URL Contains" or "Categories", or target specific URLs with "URL Equals" or "Page Feeds" [15,16]. These approaches can be summarized as follows. Dynamic Search Ads allow advertisers to target individual URLs (URL Equals), pages containing certain strings (URL Contains), or Google Ads-generated categories based on landing pages. Advertisers can also upload a page feed of URLs for more focused targeting, such as labeling pages for specific product types or availability. These technical options enable advertisers to refine their audience targeting and personalize content delivery.

4. Retargeting

This strategy involves showing ads to users who have previously interacted with a brand but haven't made a purchase. For example, if a user visits an online store and views a specific product, they may later see ads for that exact product on their social media feeds.

5. Lookalike Audiences

Advertisers can create lookalike audiences by identifying common characteristics among their existing customers. The platform then targets users who share these characteristics but haven't yet engaged with the brand.

6. Behavioral Targeting

This approach involves using a user's online behavior to predict their interests and preferences. For instance, if a user frequently searches for hiking trails and outdoor gear, they might see ads related to outdoor activities.

7. Location-Based Targeting

Social media platforms can deliver ads based on a user's geographical location. Local businesses often use this feature to target users in their vicinity with special offers or promotions.

8. A/B Testing

Advertisers can personalize advertisements and then test different versions to determine which ones perform better. This iterative process helps refine personalization strategies. An A/B test is a method of comparing two variations of an ad, piece of content, or other material to see which version performs better.

Split testing, also known as A/B testing, involves dividing the audience into two distinct groups. Each group is shown a different variation of the same advertisement. The results are then evaluated to determine which version performs most effectively [17].

Survey Results

The results of this survey play a crucial role in understanding the landscape of digital privacy, providing empirical evidence that can guide important policy decisions. By dissecting users' privacy perceptions and behaviors, stakeholders in governance, technology design, and education can work towards crafting more effective privacy protections that align with public concerns. Examining privacy perceptions and behaviors is essential due to the pervasive influence of social media platforms on personal, social, and civic life. Understanding how individuals perceive surveillance and how these perceptions influence their actions clarifies the real-world impact of platform practices and policy decisions. Insights from this analysis inform academic debates and guide platform design and policymaking, ensuring that privacy protections address genuine user concerns. This study analyzes privacy perceptions, worry levels, and behavioral intentions among social media users to elucidate the relationship between privacy concerns and protective behaviors. The research addresses gaps in quantitative studies on privacy attitudes and provides empirical evidence for policy and platform design.

Methods

Sample and Procedure

Data were collected through an anonymous Google Forms survey (N = 127) conducted in August and September 2023. The survey link was distributed through personal contacts, and participants were encouraged to forward it to others (snowball sampling). The sample comprised predominantly young adults: 40.2% aged 18–24 (n = 51), 37.0% under 18 (n = 47), with smaller proportions in older age groups. Gender distribution was balanced with 48.8% female (n = 62) and 48.8% male (n = 62) participants, plus 2.4% other/prefer not to say (n = 3).

Results

Descriptive Statistics

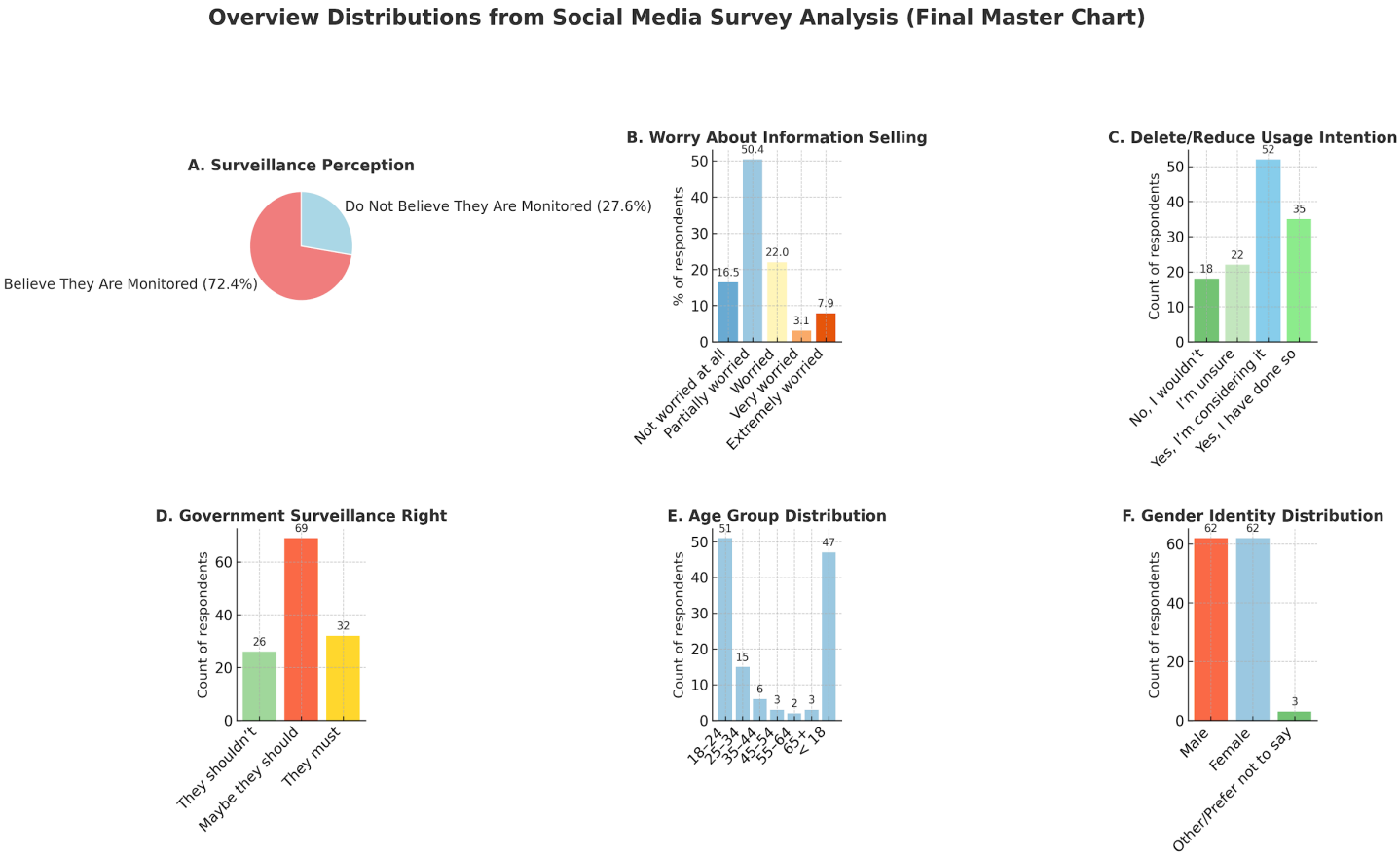
Analysis revealed high levels of awareness about surveillance among participants. The majority (72.4%, n = 92) believed their personal information and online activities are being monitored on social media platforms. Regarding concern about data selling, participants were predominantly “partially worried” (50.4%, n = 64), followed by "worried" (22.0%, n = 28), "not worried at all" (16.5%, n = 21), "extremely worried" (7.9%, n = 10), and "very worried" (3.1%, n = 4).

Behavioral intentions showed substantial engagement with privacy-protective actions. Most participants (68.5%, n = 87) indicated they have deleted or are considering deleting social media platforms due to privacy concerns, with 40.9% (n = 52) currently considering deletion and 27.6% (n = 35) having already taken action.

Variable	n	%
Age Group	Age Group	Age Group
< 18	47	37.0%
18-24	51	40.2%
25-34	15	11.8%
35+	14	11.0%
Gender Identity	Gender Identity	Gender Identity

Female	62	48.8%
Male	62	48.8%
Other/Prefer not to say	3	2.4%

Figure 1. Distribution of Key Survey Variables



Note. Panel A displays surveillance perception (Yes: 72.4%, No: 27.6%). Panel B shows concern about information selling, with “Partially worried” being the most common response (n = 64). Panel C presents deletion/reduction intentions, with 52 participants considering this option and 35 having already implemented it. Panel D illustrates government surveillance attitudes. Panels E and F display the demographic distributions for age groups and gender identity, respectively.

Statistical Tests of Independence

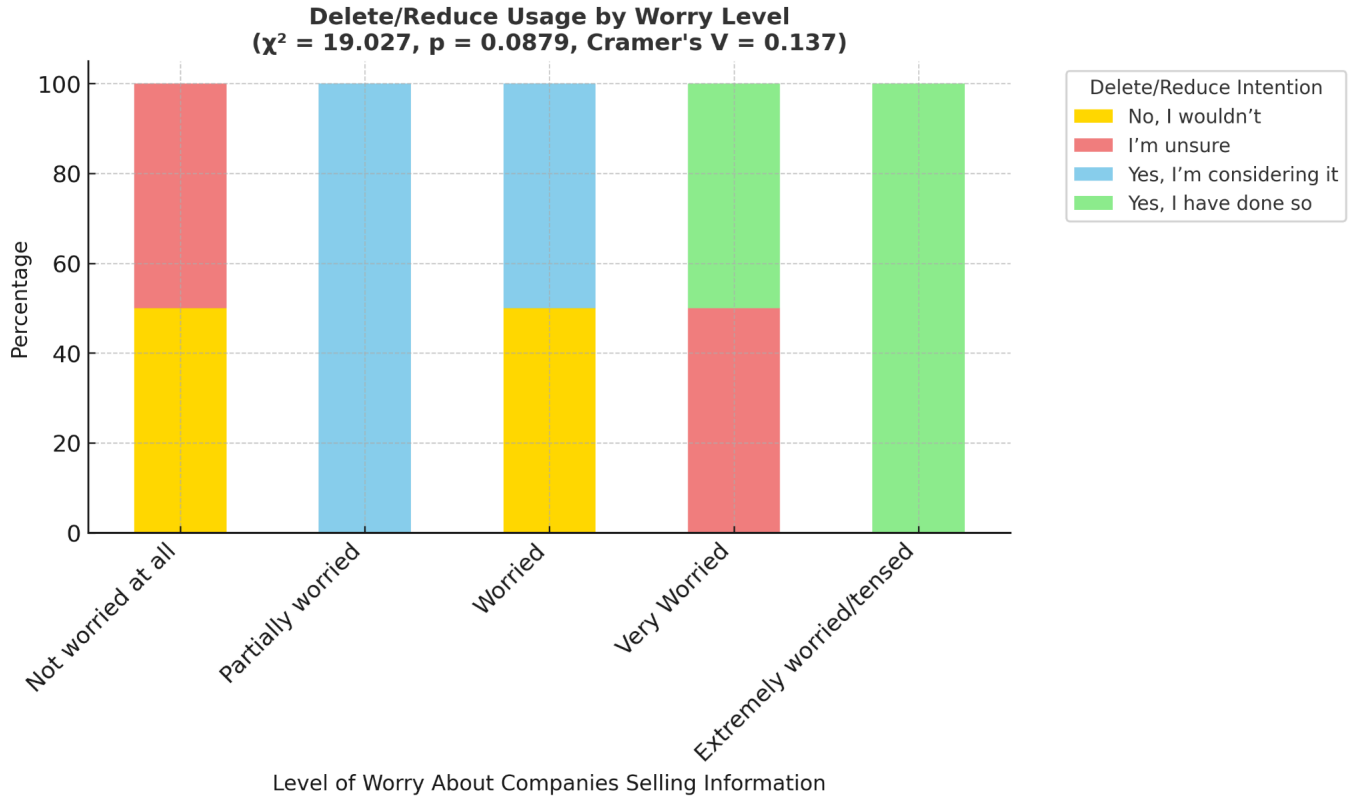
Chi-square tests examined associations between key variables using the formula:

$$\chi^2 = \Sigma[(Oij - Eij)^2 / Eij]$$

Where Oij represents observed frequencies and Eij represents expected frequencies for each cell. Three primary associations were tested:

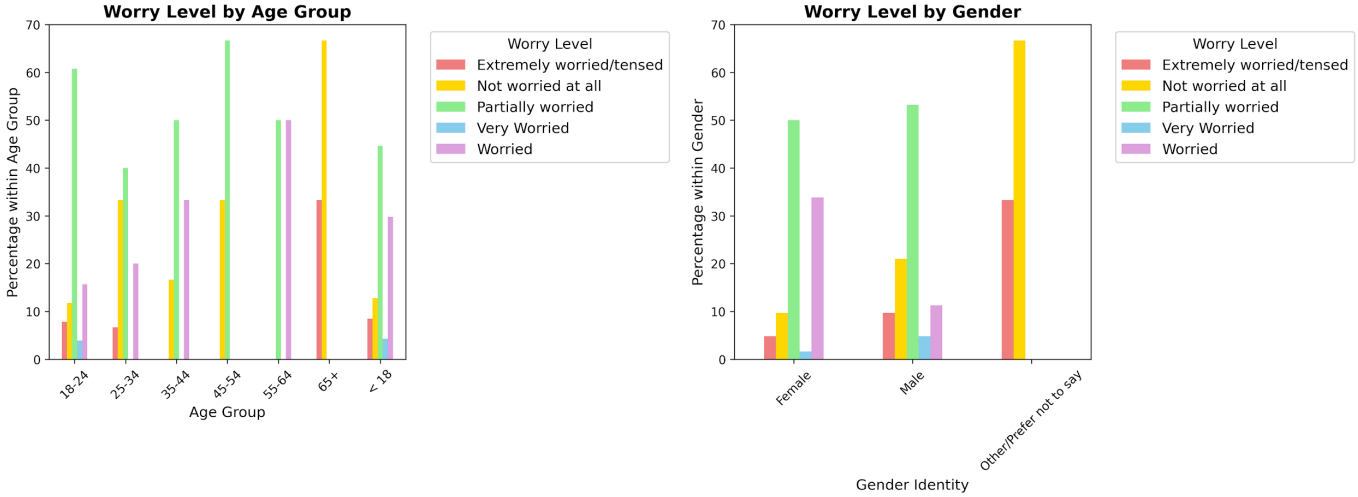
1. **Worry Level × Delete Intention:** $\chi^2(12, N = 127) = 19.027$, $p = 0.088$, Cramer's V = 0.137. The relationship between privacy worry and deletion intention approached statistical significance, suggesting a moderate association between concern levels and protective behaviors.
2. **Gender × Worry Level:** $\chi^2(8, N = 127) = 21.091$, $p = 0.007$, Cramer's V = 0.228. A statistically significant association emerged between gender identity and privacy worry levels, indicating meaningful differences in privacy concerns across gender groups.
3. **Age Group × Worry Level:** $\chi^2(24, N = 127) = 21.656$, $p = 0.600$, Cramer's V = 0.000. No significant association was found between age group and worry levels within this predominantly young sample.

Figure 2. Delete/Reduce Usage by Worry Level



Note. Stacked bar chart showing the relationship between worry levels about companies selling information (x-axis) and intention to delete or reduce platform usage (represented by different colored segments). Chi-square test results: $\chi^2 = 19.027$, $p = 0.088$, V = 0.137. The pattern suggests higher worry levels are associated with greater deletion intentions, though the relationship approached but did not reach conventional statistical significance.

Figure 3. Privacy Worry by Demographics



Note. Panel A displays worry level distributions across age groups, showing relatively consistent patterns across younger age categories. Panel B presents worry levels by gender identity, revealing a statistically significant gender difference ($\chi^2 = 21.091$, $p = 0.007$). Females showed higher proportions of "worried" responses, while males showed higher proportions of "not worried at all" responses.

Discussion

This analysis identifies significant privacy concerns among young social media users, challenging prevailing assumptions regarding generational indifference to digital surveillance. The finding that 72.4% of participants believe they are under surveillance, along with 68.5% having deleted or considering deleting platforms, indicates a high level of privacy awareness and proactive behavioral responses.

The significant gender difference in privacy worry levels ($p = .007$, $V = 0.228$) represents a notable finding with practical implications. This medium effect size suggests that privacy concerns vary systematically across gender identities, warranting further investigation into gendered experiences of digital surveillance and targeted intervention strategies. The pattern may reflect differential exposure to online harassment, varying socialization practices related to privacy, or distinct risk perceptions across gender groups.

The near-significant association between worry levels and deletion intentions ($p = .088$, $V = 0.137$) provides evidence for privacy calculus theory, suggesting that as privacy concerns increase, users become more likely to take protective actions. This relationship supports models of behavioral intention, where attitudes predict behaviors; however, the cross-sectional design limits the ability to make causal inferences.

Notably, age showed no association with privacy worry within this predominantly young sample, suggesting that privacy concerns may be more universal across younger age groups than previously assumed. This finding contradicts stereotypes about digital natives being unconcerned with privacy and supports treating young users as sophisticated decision-makers when it comes to privacy.

Study limitations include potential self-selection bias toward privacy-conscious participants, a cross-sectional design preventing causal inference, and limited demographic diversity. The convenience sampling method may not accurately represent broader populations, and self-reported behaviors may be influenced by social desirability bias.

Policy and Design Recommendations

Based on the findings of this study, several policy and design recommendations are proposed. These recommendations aim to help platforms, policymakers, and educators address privacy concerns and behaviors more effectively, as identified in the research.

1. **Platform Design:** Social media companies should implement more granular privacy controls and transparent data usage policies, recognizing that users across demographic groups express substantial privacy concerns and are willing to take protective actions.
2. **Gender-Sensitive Approaches:** Given significant gender differences in privacy concerns, platforms and policymakers should develop targeted privacy education and protection measures that address the varying needs and risk perceptions across different gender identities.
3. **Youth Privacy Rights:** Policymakers should acknowledge the sophisticated privacy concerns of young users and develop age-appropriate privacy protections that respect their autonomy while providing meaningful safeguards against surveillance and data exploitation.
4. **Digital Literacy:** Educational programs should focus on empowering users with practical privacy management skills rather than assuming indifference to privacy issues, building on existing privacy awareness to enhance protective capabilities.

Conclusion

This study examined the use of surveillance and targeted advertising by social media platforms to collect and monetize user data. Findings from 127 participants indicate that users are more privacy-aware than commonly assumed: 72.4% recognized surveillance, and 68.5% took or considered protective actions. Significant gender differences ($p = .007$) suggest that tailored strategies may be more effective than universal approaches. Beyond individual concerns, these results underscore broader power imbalances, as platforms, advertisers, and governments exert disproportionate control over personal data. Addressing these issues requires regulatory measures that extend beyond transparency, including enforceable privacy controls, data minimization standards, and youth-specific protections that acknowledge the existing level of privacy awareness among young users. Future research should investigate the causes of gender differences, track privacy attitudes over time, and compare cross-cultural variations. Evaluating practical interventions such as clearer policy designs or digital literacy initiatives will also be crucial. Continued research is essential to ensure that advancing technologies support innovation while safeguarding fundamental privacy rights. In reflecting on the “generational indifference” myth, this research clearly illustrates that younger users are more aware and proactive about privacy issues than often presumed, thereby challenging this stereotype and emphasizing the need for nuanced policy approaches. To further these efforts, how might stakeholders collaborate in developing youth-specific protections that resonate with the needs

and concerns of young users? Engaging diverse disciplines could foster the creation of holistic solutions that prioritize the privacy rights and safety of this demographic.

References

[1] Lightfoot, Geoffrey, and Tomasz Piotr Wisniewski. 2014. "Information Asymmetry and Power in a Surveillance Society." ResearchGate. https://www.researchgate.net/publication/264253929_Information_Asymmetry_and_Power_in_a_Surveillance_Society (accessed October 17, 2025).

[2] Abbas, Ghadier M. 2024. "The Influence of Political Advertising on Voter Behavior: A Study on How Targeted Ads Shape Voter Preferences and Engagement." *Interdisciplinary Journal of Humanities, Media, and Political Science* 1, no. 2. https://www.researchgate.net/publication/387647023_The_Influence_of_Political_Advertising_on_Voter_Behavior_A_Study_on_How_Targeted_Ads_Shape_Voter_Preferences_and_Engagement (accessed October 17, 2025).

[3] Brown, Iain. 2014. "Social Media Surveillance." *The International Encyclopedia of Digital Communication and Society*, 1–7. doi:10.1002/9781118767771.wbiedcs122 (accessed October 17, 2025).

[4] Fuchs, Christian. n.d. "22. Social Media Surveillance." Web archive copy of PDF. https://web.archive.org/web/20190711113414id_/http://www.fuchs.uti.at:80/wp-content/DS.pdf (accessed October 17, 2025).

[5] Insider Intelligence (Yuen, Meaghan). 2024. "Excellent CX Requires Proper Organizational Structure and Team Setup." Insider Intelligence. https://www.insiderintelligence.com/insights/customer-experience-best-practices/ (accessed October 17, 2025).

[6] Syaputra, Ringgo, and Andi Azhar. 2025. "The Effectiveness of Personalized Advertising on Consumer Engagement through Emotional Attachment on Social Media." *Paraplu Journal* 2, no. 1: 101–13. https://www.researchgate.net/publication/388001584_THE_EFFECTIVENESS_OF_PERSONALIZED_ADVERTISING_ON_CONSUMER_ENGAGEMENT_THROUGH_EMOTIONAL_ATTACHMENT_ON_SOCIAL_MEDIA (accessed October 17, 2025).

[7] Motlani, Sneha; Choudhary, Sneha; and Jain, Richa. 2025. "Customization and Personalization: Driving Engagement and Loyalty in the Digital Marketplace." *International Journal of Advances in Business and Management Research (IJABMR)*. https://ejournal.svgacademy.org/index.php/ijabmr/article/view/179 (accessed October 17, 2025).

[8] Xiph. 2022. "How social media is tracking you & collecting your data." Xiph Cyber, July 9, 2022. https://xiphcyber.com/articles/social-media-tracking (accessed October 17, 2025).

[9] Aguado, Carmen. 2012. "Facebook or Face Bank?" *Loyola of Los Angeles Entertainment Law Review* 32, no. 2: 187–95. https://digitalcommons.lmu.edu/elr/vol32/iss2/2 (accessed October 17, 2025).

[10] Schaefer, Aubree. 2023. "How to collect and mine your social media data for growth." *Sprout Social*, July 6, 2023. https://sproutsocial.com/insights/social-media-data-collection/ (accessed October 17, 2025).

[11] Audiense. 2021. “What is Social Media Audience Segmentation?: A Guide.” Audiense Resources, June 21, 2021. https://resources.audiense.com/en/blog/what-is-social-media-audience-segmentation (accessed October 17, 2025).

[12] Aguado, Carmen. 2012. "Facebook or Face Bank?" *Loyola of Los Angeles Entertainment Law Review* 32, no. 2: 187–95. https://digitalcommons.lmu.edu/elr/vol32/iss2/2 (accessed October 17, 2025).

[13] DataReportal. 2025. "Pinterest Users, Stats, Data & Trends for 2025." DataReportal – Global Digital Insights. Most recent update March 12, 2025. https://datareportal.com/essential-pinterest-stats (accessed October 17, 2025).

[14] DataReportal. 2025. "Pinterest Users, Stats, Data & Trends for 2025." DataReportal – Global Digital Insights. Most recent update March 12, 2025. https://datareportal.com/essential-pinterest-stats (accessed October 17, 2025).

[15] Google Support. n.d. "About Dynamic Search Ads." Google Ads Help. https://support.google.com/google-ads/answer/2471185?hl=en-GB (accessed December 19, 2023; accessed October 17, 2025).

[16] Dynamic Yield (Fox, Meir). 2016. “What Are Dynamic Ads / Dynamic Creatives?” Dynamic Yield glossary. https://www.dynamicyield.com/glossary/dynamic-ads/ (accessed October 17, 2025).

[17] Clark, Taylor. 2021. “How to Run A/B Tests on Social Media.” *Ignite Social Media*, July 22, 2021. https://www.ignitesocialmedia.com/social-media-marketing/how-to-run-a-b-tests-on-social-media/ (accessed October 17, 2025).

[18] Al-Malaise Al-Ghamdi, Abdullah S., and Farrukh Saleem. 2024. “Impact of Artificial Intelligence on Social Media Networks.” *Journal of Electrical Systems* 20, no. 9 (July 2024): 2112–18. https://www.researchgate.net/publication/382359490_Impact_of_Artificial_Intelligence_on_Social_Media_Networks (accessed October 17, 2025).

[19] Wiradhany, Wisnu; Pócs, Anna; and Baumgartner, Susanne E. 2024. “Are Social Media Notifications Distracting?.” *Experimental Psychology* 71, no. 4 (July 2024): 189–201. https://pubmed.ncbi.nlm.nih.gov/39552411 / (accessed October 17, 2025).

APPENDIX A: SURVEY INSTRUMENT

Question No.	Question	Response Options
1	Do you think that your personal information and online activities in social media are being watched?	Yes / No
2	How worried are you that social media companies sell your information?	Not worried at all / Partially worried / Worried / Very Worried / Extremely worried/tensed
3	How often do you read and understand the “Terms and Conditions” and “Privacy Policies” of the social media and websites & apps that you use?	No, not really / I am not sure / Yes, occasionally / Yes, frequently
4	Would you consider deleting or reducing your usage of specific social media platforms due to concerns about privacy and surveillance?	No, I wouldn't / I'm unsure / Yes, I'm considering it / Yes, I have done so
5	On what scale do you believe that government agencies have the right to conduct surveillance via social media for national security?	They shouldn't / Maybe they should / They must
6	What is your age?	Below 18 / 18 to 24 / 24 to 34 / 35 to 44 / 45 to 54 / 55 to 64 / Above 64
7	What is your gender identity?	Open text field (consolidated for analysis)

Data Processing and Coding

Ordinal variables were coded numerically, with transparent mappings documented. Multiple responses within single cells were handled by extracting the first response. Gender categories with fewer than five responses were consolidated into “Other/Prefer not to say” following standard practice. Age ranges were mapped to ordered categories for analysis.

APPENDIX B: DATA CODING DECISIONS

Variable Coding Schemes

Variable	Response Option	Numeric Code
Surveillance Perception	No	1
	Yes	2
Worry About Selling	Not worried at all	1
	Partially worried	2
	Worried	3
	Very Worried	4
	Extremely worried/tensed	5
Reading Policies	No, not really	1
	I am not sure	2
	Yes, occasionally	3
	Yes, frequently	4
Delete Intention	No, I wouldn't	1
	I'm unsure	2
	Yes, I'm considering it	3
	Yes, I have done so	4

Government Surveillance	They shouldn't	1
	Maybe they should	2
	They must	3

Additional Data Processing Decisions

Procedure	Description
Gender Consolidation	Categories with fewer than 5 responses were combined into "Other/Prefer not to say" following standard practice for statistical analysis to ensure adequate cell sizes for chi-square tests.
Multiple Response Handling	When multiple responses were found within single cells, the first response was extracted and used for analysis.
Missing Data	No imputation was performed for missing values. Cases with missing data were excluded from relevant analyses on a pairwise basis.

Statistical Analysis

Descriptive statistics included frequencies and percentages for categorical variables. Chi-square tests of independence examined associations between key variables, with Cramer's V calculated as the effect size measure. Fisher's exact test was used when expected cell frequencies fell below 5. All analyses used an $\alpha = .05$ significance level and adhered to APA reporting standards.