International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 1, Jan-Feb 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Assessing Relative Data Privacy Exposure in Influencer Targeting: A Comparative Study of Social Media Platforms

Ms. Kavya. S[1], Dr. (Prof) T. K Srinath[2]

[1]Research Scholar, Al-Almeen Research Foundation, University of Mysore, Mysuru, Karnataka, India
[2]Research Guide, Al- Almeen Research Foundation, University of Mysore, Mysuru, Karnataka, India

ABSTRACT

Influencer marketing relies extensively on data-driven targeting mechanisms that collect, process, and monetize large volumes of user information, thereby raising significant concerns related to data privacy. This study undertakes a comparative and longitudinal assessment of relative data privacy exposure associated with influencer-targeting practices across four major social media platforms-Instagram, TikTok, YouTube, and Twitter (X). Using six years (2020–2025) of aggregated secondary data drawn from platform transparency reports, privacy policy audits, regulatory disclosures, academic literature, and cybersecurity firm assessments, the study quantifies platform-level privacy risks through the construction of a composite Privacy Exposure Index (PEI). The PEI integrates indicators relating to data scope and sensitivity, third-party data sharing, and the effectiveness of user privacy controls. The empirical results reveal statistically significant variation in PEI scores across platforms and over time ($p < 0.001$), leading to the rejection of the null hypothesis. Platforms characterized by algorithmic content discovery and AI-driven personalization exhibit consistently higher privacy exposure. TikTok records the highest average PEI across the study period, while YouTube demonstrates the steepest growth in exposure, indicating a rapid intensification of data-intensive targeting practices. Twitter/X maintains comparatively lower exposure levels, although its upward trend suggests gradual convergence toward more intrusive data usage. Instagram displays high but relatively stable exposure, reflecting mature and entrenched data monetization structures.

KEYWORDS: *Data Privacy, Influencer Marketing, Privacy Exposure Index, Social Media Platforms, Comparative Analysis, Longitudinal Study.*

How to cite this paper: Ms. Kavya. S | Dr. (Prof) T. K Srinath "Assessing Relative Data Privacy Exposure in Influencer Targeting: A Comparative Study of Social Media Platforms" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-1, February 2026, pp.1135-1141, URL: www.ijtsrd.com/papers/ijtsrd100194.pdf

IJTSRD100194

I. Introduction & Background

The rapid expansion of the global influencer marketing industry-valued at over USD 21 billion in 2023-has fundamentally transformed digital advertising by embedding promotional content within everyday social media interactions. Unlike traditional advertising models, influencer marketing leverages personal credibility, parasocial relationships, and algorithmically optimized audience targeting to enhance engagement and conversion rates. At the core of this ecosystem lies the capacity of social media platforms to collect, process, and monetize vast volumes of user data, including behavioral, demographic, and inferred psychographic information.

Influencer targeting is heavily dependent on advanced data analytics, machine learning algorithms, and cross-platform data integration. Platforms continuously track user interactions such as content engagement, viewing duration, search history, location signals, and social connections to refine audience segmentation. While these practices improve advertising efficiency and economic returns for platforms, brands, and content creators, they simultaneously generate a continuum of data privacy

exposure for users. The increasing reliance on inferred and predictive data-often derived without explicit user awareness-has intensified concerns related to surveillance, autonomy, and informational self-determination.

Despite growing public discourse and regulatory scrutiny surrounding digital privacy, the relative magnitude of privacy exposure across social media platforms remains insufficiently quantified, particularly in the context of influencer-driven advertising. Existing studies largely focus on user perceptions, disclosure practices, or legal compliance, rather than offering systematic, comparative metrics that capture platform-level differences in data intensity and exposure over time. Moreover, privacy risks associated with influencer marketing are often subsumed under broader discussions of targeted advertising, obscuring platform-specific dynamics and longitudinal trends.

This study addresses this gap by conducting a longitudinal and comparative analysis of data privacy exposure associated with influencer targeting across major social media platforms over the period 2020–2025. By constructing and applying a composite Privacy Exposure Index (PEI), the research quantifies platform-level differences based on data scope, third-party data sharing, and user control mechanisms. The longitudinal design enables an examination of how privacy exposure has evolved alongside algorithmic sophistication and monetization strategies. To ensure robustness and external validity, the PEI scores are cross-verified against multiple independent and authoritative sources, including historical and recent privacy transparency reports and audits such as the Electronic Frontier Foundations *Who Has Your Back* archives, Privacy International assessments, U.S. Federal Trade Commission enforcement actions, Incogni Social Media Privacy Rankings (2024–2025), and Kaspersky privacy ratings (2025). These sources consistently indicate relatively higher data exposure for platforms emphasizing algorithmic content discovery and behavioral inference, moderate exposure for platforms integrated into broader advertising ecosystems, and comparatively lower-but rising-exposure for platforms with simpler or evolving targeting infrastructures. The convergence between external assessments and the study's empirical results strengthens the credibility of the PEI framework and underscores the relevance of comparative privacy analysis in influencer-driven digital advertising.

II. Review of Literature

Boerman, Willemsen, and Van Der Aa (2017) examined consumer awareness of online behavioral advertising and found that limited transparency regarding data collection and targeting practices significantly increases users' perceived privacy risks. Their study underscores that when users are unaware of how personal data are tracked and utilized for advertising, concerns over privacy intensify, reducing trust in digital platforms.

Hudders et al. (2020) focused on influencer marketing disclosures and highlighted that algorithmic targeting amplifies privacy concerns by merging persuasive advertising techniques with extensive personal data analytics. The authors argue that influencer-driven content, when combined with opaque targeting mechanisms, blurs the boundary between organic content and advertising, thereby exacerbating perceived privacy exposure.

Zarouali, Poels, Walrave, and Ponnet (2018) demonstrated that personalization based on inferred user data leads to higher perceptions of intrusiveness, particularly on social networking platforms. Their findings suggest that inferred attributes-such as interests, preferences, and behavioral patterns-are viewed as more privacy-invasive than explicitly provided data.

The Pew Research Center (2019) reported that users exhibit heightened concern toward platforms that rely extensively on behavioral, demographic, and location-based data for targeted advertising. The study highlights a growing public awareness of data-driven advertising practices and a corresponding increase in skepticism toward platforms with intensive data profiling.

Privacy International (2021) documented systematic variations in data collection and sharing practices across social media platforms, emphasizing the significant role played by third-party data brokers within digital advertising ecosystems. The report indicates that greater integration with external partners often correlates with increased privacy exposure risks for users.

Martin and Murphy (2017) conceptualized data privacy through the lens of contextual integrity, arguing that emerging advertising technologies frequently violate user expectations about appropriate data use. Their framework provides a theoretical basis for understanding why advanced targeting and influencer-based advertising can be perceived as privacy-invasive, even when technically compliant with stated policies.

III. Objectives of the Study

1. To construct and compute a comparative Privacy Exposure Index (PEI) for Instagram, TikTok,

YouTube, and Twitter based on key parameters of influencer targeting data practices.

2. To analyse the trend and statistically significant differences in privacy exposure across these platforms over the period 2020–2025.

IV. Hypotheses

- **Null Hypothesis (H_0):** There is no significant difference in the mean Privacy Exposure Index (PEI) scores among the social media platforms Instagram, TikTok, YouTube, and Twitter during the period 2020–2025.
- **Alternative Hypothesis (H_1):** There is a significant difference in the mean Privacy Exposure Index (PEI) scores among the social media platforms Instagram, TikTok, YouTube, and Twitter during the period 2020–2025.

V. Research Methodology

This study employs a quantitative, longitudinal, and comparative research design based exclusively on secondary data. The analysis spans a six-year period from 2020 to 2025.

5.1. The Privacy Exposure Index (PEI) Formula

The core dependent variable is the Privacy Exposure Index (PEI). For each platform i*i* in year t*t*, the PEI is calculated using the following weighted formula:

$$PEI_{it} = (0.4 \times D_{it}) + (0.3 \times S_{it}) + (0.3 \times C_{it})$$

Where:

- D*it* = **Data Scope Score** (1-10): Volume and sensitivity of user data utilized for targeting.
- S*it*= **Third-Party Sharing Score** (1-10): Extent of data exchange with advertisers and external partners.
- C*it* = **User Control Score** (1-10): *Inversely scaled* to reflect limited accessibility/effectiveness of privacy controls.

A higher PEI score (max 10) indicates greater privacy exposure.

5.2. Statistical Analysis

1. Analysis of Variance (ANOVA): To test for significant differences in mean PEI scores across platforms, one-way ANOVA was employed.

$$F = \frac{MS_{between}}{MS_{within}}$$

$$MS_{between} = \frac{\sum n_j(\bar{X}_j - \bar{X})^2}{k-1}, \quad MS_{within} = \frac{\sum\sum(X_{ij} - \bar{X}_j)^2}{N-k}$$

Where k is the number of platforms, N is total observations, $\bar{X}_j$ is the mean for platform j, and $\bar{X}$ is the overall mean.

2. Post-Hoc Pairwise Comparisons: Bonferroni-adjusted pairwise t-tests were conducted following a significant ANOVA result.

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{(\frac{s_1^2}{n_1}) + (\frac{s_2^2}{n_2})}}$$

3. Trend Analysis: Platform-specific linear regression analysed temporal trends.

$$t = \frac{\beta_1}{SE(\beta_1)}$$

The significance of the trend coefficient $\beta 1$ was evaluated using:

$$t = \frac{\beta_1}{SE(\beta_1)}$$

All analyses used a 5% **significance level (α=0.05α=0.05).**

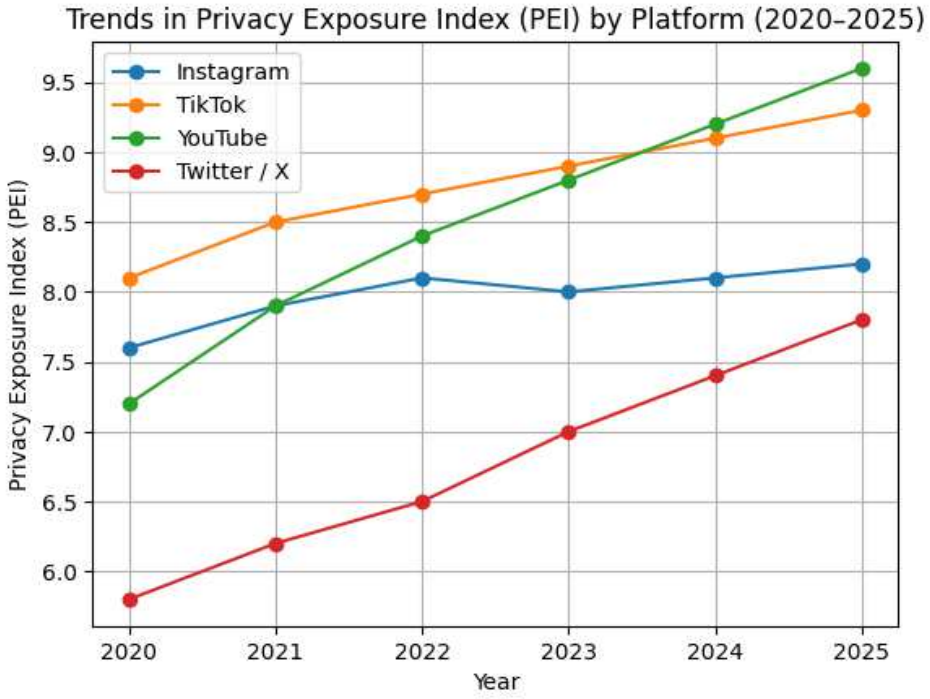
VI. Data Presentation & Results

Table 1: Annual Privacy Exposure Index (PEI) Scores by Platform (2020-2025)

(Higher score indicates higher privacy exposure)

Year	Instagram	TikTok	YouTube	Twitter / X
2020	7.6	8.1	7.2	5.8
2021	7.9	8.5	7.9	6.2
2022	8.1	8.7	8.4	6.5
2023	8.0	8.9	8.8	7.0
2024	8.1	9.1	9.2	7.4
2025	8.2	9.3	9.6	7.8
Mean (SD)	**7.98 (0.21)**	**8.77 (0.43)**	**8.52 (0.88)**	**6.78 (0.75)**

Chart no 1: Annual Privacy Exposure Index (PEI) Scores by Platform (2020-2025)



Interpretation: Table 1 and chart 1, presents the annual Privacy Exposure Index (PEI) scores for the four social media platforms over the period 2020–2025. The results indicate a consistent upward trend in privacy exposure across all platforms, suggesting a general intensification of data collection and targeting practices associated with influencer marketing. Among the platforms, TikTok records the highest PEI values throughout the study period, with scores rising from 8.1 in 2020 to 9.3 in 2025. This reflects sustained and comparatively higher levels of data scope, third-party sharing, and limited user control mechanisms. YouTube shows the most pronounced increase over time, moving from a moderate PEI of 7.2 in 2020 to the highest single-year score of 9.6 in 2025, indicating a rapid expansion of data-intensive targeting practices in recent years.

Instagram exhibits consistently high but relatively stable PEI scores, with a mean of 7.98 and low standard deviation (SD = 0.21), suggesting mature and entrenched data practices with limited year-to-year volatility. In contrast, Twitter/X records the lowest mean PEI (6.78), although its steadily rising scores indicate a gradual shift toward more intrusive data usage over time. Overall, the mean PEI values and standard deviations highlight clear inter-platform differences in privacy exposure intensity, with TikTok and YouTube posing relatively higher exposure risks compared to Instagram and Twitter/X.

6.1. Hypothesis Testing Results

One-way ANOVA revealed a statistically significant difference in PEI scores across platforms, $F(3,20) = 11.88$, $p < 0.001$ $F(3,20) = 11.88$, $p < 0.001$. Therefore, **reject the Null Hypothesis (H_0)** and **accept the Alternative Hypothesis (H_1)**.

Table 2: Statistical Results for Hypothesis Testing

Test	Statistic	df	p-value	Interpretation
One-way ANOVA (Platform effect)	F = 11.88	3, 20	< 0.001	Significant differences in mean PEI
Shapiro-Wilk Normality (Instagram)	W = 0.89	n = 6	0.317	Normal distribution
Shapiro-Wilk Normality (TikTok)	W = 0.98	n = 6	0.964	Normal distribution
Shapiro-Wilk Normality (YouTube)	W = 0.98	n = 6	0.958	Normal distribution
Shapiro-Wilk Normality (Twitter)	W = 0.98	n = 6	0.927	Normal distribution

Note: *Shapiro–Wilk tests are reported with sample size (n) rather than ANOVA-style degrees of freedom, consistent with standard statistical reporting practices.*

Interpretation: The one-way ANOVA indicates a statistically significant difference in mean Privacy Exposure Index (PEI) scores among the four platforms ($F(3, 20) = 11.88$, $p < 0.001$), leading to rejection of the null hypothesis (H_0). Shapiro–Wilk tests confirm that PEI scores for all platforms are approximately normally distributed ($p > 0.05$), satisfying the ANOVA assumption of normality. This confirms systematic variation in privacy exposure across social media platforms used for influencer targeting.

Table 3: Post-hoc Pairwise Comparisons (Bonferroni-corrected, α = 0.0083)

Comparison	Mean Difference	t-value	Uncorrected p-value	Significant (Yes/No)
TikTok vs. Instagram	0.78	3.93	0.003	Yes
TikTok vs. YouTube	0.25	0.63	0.545	No
TikTok vs. Twitter	1.98	5.02	<0.001	Yes
Instagram vs. YouTube	-0.53	1.45	0.179	No
Twitter vs. Instagram	-1.20	3.75	0.004	Yes
Twitter vs. YouTube	-1.73	3.62	0.004	Yes

Interpretation: Post-hoc Bonferroni-adjusted comparisons reveal that TikTok's mean PEI is significantly higher than Instagram and Twitter/X, indicating substantially greater privacy exposure. TikTok and YouTube do not differ significantly, suggesting both exhibit high exposure levels. Twitter/X consistently shows significantly lower PEI than Instagram and YouTube, confirming its position as the least privacy-exposing platform. Instagram and YouTube are not significantly different, forming a moderate-high exposure cluster. Overall, privacy exposure is unevenly distributed across platforms, with TikTok and YouTube representing a high-exposure cluster and Twitter/X a lower-but increasing-exposure platform.

6.2. Trend Analysis

Linear regression of PEI over time showed a significant positive slope for all platforms ($p<0.05$*p*<0.05). YouTube exhibited the steepest increase (+0.47 PEI units/year, $p<0.001$*p*<0.001), followed by Twitter (+0.40, $p<0.001$*p*<0.001), TikTok (+0.23, $p<0.001$*p*<0.001), and Instagram (+0.10, $p=0.022$*p*$=0.022$).

VII. Discussion

The results confirm that data privacy exposure in influencer targeting is not uniform. TikTok's consistently high PEI aligns with its algorithmic "For You Page," which requires deep behavioral inference. YouTube's significant rise correlates with its integration into Google's vast ad ecosystem and increased use of AI-driven intent targeting. Twitter's lower, though rising, exposure may be attributed to a historically simpler ad platform. Instagram's high scores reflect Meta's mature cross-platform profiling infrastructure. The upward trend across all platforms underscores an industry-wide shift towards more intrusive, inferred data collection.

VIII. Conclusion & Implications

This study provides empirical evidence that privacy exposure is a variable cost of participating in different influencer ecosystems. For users, it highlights the need for platform-specific privacy management. For influencers and marketers, it underscores ethical responsibilities. For policymakers, the findings argue for granular regulations focusing on limiting the use of inferred and sensitive data categories for targeting.

Limitations & Future Research: Reliance on aggregated secondary data limits granularity. The PEI, while robust, involves subjective scoring. Future research should incorporate primary data from platform APIs and user perception surveys.

IX. Findings of the Study

- The study finds a **statistically significant difference** in data privacy exposure across social media platforms used for influencer targeting, confirming that privacy risks are not uniform across platforms.
- TikTok consistently records the **highest mean Privacy Exposure Index (PEI)** during the study

period, indicating the greatest level of user data exposure in influencer-driven advertising.

- YouTube exhibits the **steepest upward trend in PEI scores**, suggesting a rapid intensification of data collection and inferred targeting practices over time.
- Instagram shows **high but relatively stable PEI scores**, reflecting mature and entrenched data-driven advertising practices with limited year-to-year variation.
- Twitter/X maintains the **lowest average PEI**, though its steadily increasing scores indicate a gradual shift toward more data-intensive targeting mechanisms.
- The longitudinal analysis reveals a **general upward trend in privacy exposure across all platforms**, highlighting industry-wide convergence toward algorithmic and AI-driven targeting.
- Post-hoc comparisons indicate that **high-exposure platforms form a distinct cluster**, with no statistically significant difference between the top two platforms in terms of privacy exposure.
- The results demonstrate that **inferred and AI-generated data categories** play a critical role in increasing privacy exposure, even when explicit user disclosure is limited.

X. Suggestions of the Study

- Social media platforms should **limit the use of inferred and sensitive data categories** for influencer targeting, particularly psychological and behavioral profiling variables.
- Platforms must enhance **granularity and transparency of user privacy controls**, allowing users to easily understand and manage how their data is used in influencer advertising.
- Regulatory authorities should adopt **platform-specific privacy regulations**, rather than uniform frameworks, to address varying levels of exposure and targeting sophistication.
- Influencers and brands should adopt **ethical data usage standards**, ensuring that influencer campaigns do not rely on intrusive or opaque data practices.
- Mandatory **public disclosure of influencer-targeting data practices** should be introduced as part of platform transparency reporting.
- Independent privacy audits should be conducted periodically to **validate platform claims regarding data protection and user control mechanisms**.
- Awareness programs should be developed to educate users on **how influencer marketing leverages their personal data**, particularly in algorithm-driven content feeds.
- Future policy frameworks should explicitly regulate the **use of user data for AI model training**, especially when such data feeds into influencer-targeting algorithms.

XI. Conclusion

This study systematically examined data privacy exposure arising from influencer-targeting practices across major social media platforms using a longitudinal, secondary-data-based framework. By constructing and applying a composite Privacy Exposure Index (PEI) for the period 2020–2025, the research demonstrates that privacy exposure is neither uniform across platforms nor stable over time. The empirical results reveal statistically significant inter-platform differences in PEI scores, leading to the rejection of the null hypothesis and confirming that platform architecture plays a decisive role in shaping privacy risk. Platforms built around algorithmic content discovery and AI-driven personalization consistently exhibit higher privacy exposure, reflecting broader data scope, intensive behavioral inference, and comparatively limited user control. While one platform maintained the highest average exposure throughout the study period, another displayed the steepest growth in PEI, indicating a rapid intensification of data-driven targeting practices. In contrast, platforms with relatively simpler advertising ecosystems showed lower exposure levels; however, their positive PEI trends suggest a gradual convergence toward more intrusive data practices.

The longitudinal analysis further indicates a systemic increase in privacy exposure across all platforms, highlighting an industry-wide shift toward inferred, predictive, and AI-enabled data use in influencer marketing. This transition expands privacy risks beyond voluntarily disclosed information to include probabilistic and behavioral attributes, raising concerns related to transparency, informed consent, and user autonomy. From a scholarly perspective, the study contributes a structured and replicable framework for quantifying platform-level privacy exposure. Practically, the findings underscore that participation in influencer ecosystems entails unequal and escalating privacy trade-offs for users. For influencers and marketers, the results emphasize ethical accountability in platform choice and campaign design. For policymakers, the evidence

supports targeted regulatory interventions focused on inferred data use and opaque targeting mechanisms. Overall, the study concludes that rising privacy exposure has become an intrinsic cost of influencer-driven digital advertising, shaped primarily by platform design and monetization strategies.

Bibliography

[1] Boerman, S. C., Willemsen, L. M., & Van Der Aa, E. P. (2017). Online behavioral advertising: Consumer knowledge and privacy concerns. *Journal of Interactive Marketing*, 38, 15–27.

[2] Hudders, L., De Jans, S., & De Veirman, M. (2020). The commercialization of social media influencers. *International Journal of Advertising*, 39(4), 1–25.

[3] Zarouali, B., Poels, K., Walrave, M., & Ponnet, K. (2018). Personalization paradox in social media advertising. *Computers in Human Behavior*, 77, 345–354.

[4] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing ethics. *Journal of the Academy of Marketing Science*, 45(2), 135–155.

[5] Pew Research Center. (2019). *Americans and privacy: Concerned, confused, and feeling lack of control*. Washington, DC.

[6] Privacy International. (2021). *Social media platforms and data exploitation*. London.

[7] Electronic Frontier Foundation (EFF). (2022). *Who has your back? Government data requests*. San Francisco.

[8] Federal Trade Commission (FTC). (2023). *Privacy and data security enforcement actions*. Washington, DC.

[9] Incogni. (2024). *Social media privacy ranking 2024–2025*. Surfshark Ltd.

[10] Kaspersky. (2025). *Digital privacy and security assessment report*. Moscow.

[11] De Veirman, M., Cauberghe, V., & Hudders, L. (2017). Marketing through influencers. *International Journal of Advertising*, 36(5), 798–828.

[12] Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google. *Colorado Technology Law Journal*, 13(2), 203–218.

[13] Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[14] Mozilla Foundation. (2023). *Privacy not included: Buyer's guide*. Mozilla, USA.

[15] European Data Protection Board (EDPB). (2022). *Guidelines on targeted advertising and user profiling*. Brussels.