ISSN: 2473-4901
v12 n6803

Silent Stalkers: Platform Involvement in Cyberstalking and Digital Harassment

Joveline Pettus
jovelinepettus@gmail.com
Robert Morris University
Pittsburgh, PA

Abstract

Cyberstalking and digital harassment represent growing threats to personal safety and psychological well-being in digital environments. This study addressed the following research question: Do self-identified cyberstalking victims and non-victims differ significantly in their involvement with specific categories of online platforms, social media, communication platforms, and gaming environments? Using a quantitative cross-sectional survey design, data were collected from 186 adult participants across the United States through SurveyMonkey Audience in September 2025. Of the 186 participants, 44 provided a valid response to the cyberstalking identification question and were included as the analysis subsample. Fisher's Exact tests examined associations between platform involvement and victimization status. Results indicated statistically significant associations for all three platform categories, with communication platforms producing the largest effect ($p = .003$, $\varphi = .472$). Additionally, 72.7% of participants viewed existing safety protocols as inadequate. These findings contribute inferential evidence (distinct from prior descriptive work) that specific platform categories are statistically associated with cyberstalking victimization, with implications for platform governance, digital safety policy, and information systems education.

Keywords: cyberstalking, digital harassment, platform involvement, online safety, Fisher's Exact Test

Silent Stalkers: Platform Involvement in Cyberstalking and Digital Harassment

Joveline Pettus

1. INTRODUCTION

The rapid expansion of digital communication platforms has fundamentally altered the landscape of cyberstalking and digital harassment. Unlike traditional stalking, which is bounded by physical proximity, cyberstalking exploits the architecture of digital platforms to enable persistent, cross-platform harassment that is difficult to escape, document, or prosecute (Dreßing et al., 2014). As perpetrators exploit specific platform features, anonymity in gaming environments, persistent messaging in communication applications, public profile searchability on social media, the need to examine platform-specific risk has grown increasingly urgent.

Recent systematic reviews have begun to map the landscape of cyberstalking perpetration methods, finding that platform environments are not interchangeable, specific platform features enable distinct forms of harassment (Weekes et al., 2025). Social media platforms facilitate harassment through public profile access and geolocation metadata; communication platforms enable persistent contact through direct messaging; and gaming environments introduce unique risks through real-time voice interaction and username tracking (Holt & Bossler, 2015; Fissel et al., 2024). Despite this growing descriptive literature, prior research has rarely tested whether platform involvement differs statistically between those who identify as cyberstalking victims and those who do not.

This study addresses that gap with the following research question: Do self-identified cyberstalking victims and non-victims differ significantly in their involvement with specific categories of online platforms? The findings contribute inferential evidence to a literature that has relied primarily on descriptive characterizations of platform involvement, and have direct implications for platform governance, digital safety policy, and information systems education.

2. BACKGROUND AND LITERATURE REVIEW

2.1 Cyberstalking and Digital Harassment

Cyberstalking is broadly defined as the repeated use of electronic communications to harass, threaten, or monitor an individual without their consent (Kaur et al., 2021). It encompasses persistent unsolicited digital communication, unwanted surveillance and location tracking, the creation and distribution of manipulated or synthetic media, and the unauthorized disclosure of personal information known as doxxing (Stevens et al., 2021). Research consistently documents significant psychological harm including elevated anxiety, depression, and fear (Dreßing et al., 2014; Fissel et al., 2024). Women and racial minorities are disproportionately represented among victims, while perpetration is associated with motivated offenders exploiting the structural absence of effective digital guardianship (Navarro & Jasinski, 2012; Stevens et al., 2021).

2.2 Platform-Specific Research and the Current Gap

Weekes et al. (2025), in the most comprehensive recent systematic review of cyberstalking perpetration methods, identified specific platform features as central to understanding how harassment is structured and sustained. Their analysis found that the technical affordances of platforms (not merely their category) shape perpetration patterns: anonymity features in gaming and messaging environments lower barriers to harassment, while persistent profile visibility on social media enables long-term surveillance of targets. Fissel et al. (2024) similarly found that emotional responses to cyberstalking varied by the platform context in which harassment occurred, suggesting that platform architecture mediates victim experience.

Prior to these recent contributions, the predominant approach in platform-related cyberstalking research was descriptive, documenting which platforms appeared in victim accounts without testing statistical associations between platform involvement and victimization status (Reyns et al., 2011; Lenhart et al., 2016). This descriptive tradition limits the ability to identify which platform environments represent the greatest risk, constraining the development of targeted interventions by platform operators and policymakers.

This study addresses that limitation by testing whether victims and non-victims differ statistically in their involvement across three platform categories: social media, communication, and gaming. This approach complements the feature-level analysis of Weekes et al. (2025) by providing population-level inferential evidence about which platform categories are most strongly associated with victimization.

2.3 Platform Features That Enable Harassment

The theoretical basis for platform category differences in harassment risk lies in the specific affordances each environment provides to motivated offenders. Social media platforms combine public profile visibility, searchability, location metadata, and direct messaging, creating conditions in which targets can be identified, monitored, and contacted persistently (Marwick & boyd, 2011). Communication platforms enable harassment through the highest-intensity perpetration vector: direct, private, and often anonymous persistent messaging that is difficult for platforms to moderate and for victims to escape (Weekes et al., 2025). Gaming environments introduce a distinctive risk profile through real-time voice interaction, in-game location tracking, and community-based social structures that can be weaponized against specific players (Holt & Bossler, 2015).

Media Ecology Theory (McLuhan, 1964) provides a theoretical foundation for understanding why these platform categories differ in their harassment risk: each medium embeds within its architecture a set of assumptions about identity, communication, and social interaction that shape the behaviors it enables. From this perspective, the grouping of platforms into social media, communication, and gaming categories is not arbitrary, it reflects meaningful differences in the technical affordances and social norms each environment provides to both perpetrators and victims.

2.4 Safety Protocols and Victim Support

Research consistently documents that cyberstalking victims face significant barriers to both platform-level and legal recourse. Citron (2023) argues that existing legal frameworks are fragmented and inconsistently enforced. Platform moderation policies have been criticized for prioritizing engagement over user safety, producing environments in which capable guardianship is systematically absent (Holt & Bossler, 2015). Help-seeking rates among victims are strikingly low, with prior studies finding that the majority of victims do not report their experiences or seek formal support (Dreßing et al., 2014; Stevens et al., 2021).

3. METHODOLOGY

3.1 Research Design, Sample, and Research Question

This study addressed the following research question: Do self-identified cyberstalking victims and non-victims differ significantly in their involvement with social media platforms, communication platforms, and gaming environments? A quantitative cross-sectional survey design was employed. Data were collected in September 2025 through SurveyMonkey Audience, a crowdsourced online panel providing access to a nationally distributed U.S. adult sample. The survey instrument consisted of 35 questions developed based on the existing cyberstalking and digital harassment literature, addressing participant demographics, cyberstalking victimization experiences, platform involvement, behavioral responses, emotional impact, and perceptions of safety protocol adequacy (the full survey instrument is provided in Appendix A).

Of 373 individuals who initiated the survey, 186 completed all demographic and screening questions and constituted the final analytic sample (N = 186). The 187 who did not complete the full survey were excluded due to dropout before reaching the screening question. Of the 186 who completed the survey, 44 provided a valid Yes or No response to the cyberstalking identification question, "Have you personally experienced persistent, unsolicited digital communication (e.g., messages, emails, social media interactions) that caused emotional distress or concern for your safety?", and formed the analysis subsample for all inferential analyses (n = 44), comprising 15 self-identified victims and 29 non-victims. The remaining 142 did not respond to this question due to the survey's optional response design, which was implemented to minimize participant distress when addressing sensitive victimization experiences. The critical distinction is that all 186 completed the survey's platform involvement questions, but inferential comparisons of victims versus non-victims were conducted only among the 44 who answered the cyberstalking identification question and could be classified accordingly.

3.2 Measures

Platform involvement was assessed through a survey question asking participants to identify which online platforms had been involved in incidents of cyberstalking or harassment they experienced, and how frequently harassment occurred on each. Responses were aggregated into three binary categorical variables reflecting meaningfully distinct platform architectures and harassment affordances: social media platforms (Facebook, Instagram, TikTok, Twitter/X, Reddit, Discord, Twitch), communication platforms (email, SMS/text, WhatsApp/Snapchat, anonymous platforms), and gaming platforms (Xbox Live, PlayStation Network, Steam, mobile games). Each variable was coded 1 = platform category involved, 0 = not involved. These categories reflect the theoretical distinctions established in Section 2.3, each represents a distinct set of platform features and social norms that shape harassment risk differently. Victimization status was derived from the cyberstalking identification question, coded 1 = victim and 0 = non-victim, and served as the primary grouping variable for all inferential analyses.

3.3 Analytical Approach

Fisher's Exact tests of independence were conducted to examine whether platform involvement differed significantly between victims and non-victims across each of the three platform categories. Fisher's Exact Test was selected over Pearson chi-square because preliminary assumption checks confirmed that more than 20% of cells in each contingency table had expected counts below five, violating the chi-square distributional assumption (McHugh, 2013). Phi (φ) was calculated as the effect size measure, with benchmarks of .10, .30, and .50 representing small, medium, and large effects (Cohen, 1988). Statistical significance was evaluated at α = .05. All analyses were conducted using IBM SPSS Statistics Version 29. It is important to note that these analyses establish statistical association between platform category involvement and victimization status, they do not establish causation. Platform involvement reflects participants' self-reported experience and does not indicate that platform use caused victimization.

4. RESULTS

4.1 Platform Prevalence (Descriptive)

Descriptive analysis of the full sample (N = 186) indicated that Facebook generated the highest daily harassment rate among active users (49.46%), followed by SMS/text messaging (44.62%) and email (43.75%). These rates reflect the proportion of respondents who reported daily harassment on each platform, among those who selected that platform. Gaming platforms including Xbox Live and Discord also showed substantial daily harassment rates. Harassment was not concentrated on a single platform type but was distributed across social media, communication, and gaming environments simultaneously, consistent with Weekes et al.'s (2025) finding that cyberstalking perpetrators typically employ multiple platform environments.

4.2 Platform Involvement by Victimization Status

Addressing the study's research question, Fisher's Exact tests revealed statistically significant associations between victimization status and all three platform categories (see Table 1). For social media platforms, 93.3% of self-identified victims reported involvement compared with 55.2% of non-victims, Fisher's Exact $p = .015$, $\varphi = .388$, a medium-to-large association. For communication platforms, 93.3% of victims reported involvement compared with 44.8% of non-victims, Fisher's Exact $p = .003$, $\varphi = .472$, the largest association observed and consistent with Weekes et al.'s (2025) identification of direct messaging as the highest-intensity perpetration vector. For gaming platforms, 80.0% of victims reported involvement compared with 41.4% of non-victims, Fisher's Exact $p = .025$, $\varphi = .368$. These associations are statistically significant and practically meaningful in magnitude; they do not, however, establish that platform use caused victimization or that non-victims on these platforms face equivalent risk.

Platform Category	*Non-Victim % Involved*	*Victim % Involved*	*χ^2*	*Fisher's p*	*φ*
Social Media	55.2%	93.3%	6.64	.015*	.388
Communication	44.8%	93.3%	9.81	.003**	.472
Gaming	41.4%	80.0%	5.95	.025*	.368

Table 1. Fisher's Exact Tests: Platform Involvement by Victimization Status (n = 44)
*p < .05. **p < .01. χ^2 reported for transparency; Fisher's Exact is the primary test. φ = phi coefficient. Associations reflect self-reported platform involvement and victimization status, not platform-caused victimization.

4.3 Safety Protocol Perceptions

Of the 44 participants, 72.7% indicated that existing safety protocols do not adequately address cyberstalking and digital harassment. This skepticism was shared equally by victims (73.3%) and non-victims (72.4%), suggesting broad distrust of platform and legal protections that is not limited to those with direct victimization experience.

5. DISCUSSION AND CONCLUSIONS

Addressing the study's research question, the analysis found statistically significant associations between victimization status and all three platform categories. Communication platforms produced the strongest association ($\varphi = .472$), consistent with Weekes et al.'s (2025) finding that direct messaging represents the primary perpetration vector in cyberstalking. Social media and gaming platforms also produced significant medium-to-large associations, underscoring that cyberstalking is a multi-platform phenomenon.

The platform category groupings used in this study reflect meaningful differences in platform affordances. Communication platforms' direct messaging features enable the persistent, private contact that defines cyberstalking. Social media platforms' public profile architecture facilitates surveillance and identification of targets. Gaming environments' real-time interaction and community structures create conditions for organized harassment. Future research should examine whether specific features within these categories (such as anonymity settings, direct message filtering options, or location-sharing controls) account for differential risk within platform categories, building on the feature-level analysis framework advanced by Weekes et al. (2025).

It is important to distinguish what these findings do and do not establish. The statistically significant associations between platform category involvement and victimization status indicate that victims are substantially more likely than non-victims to report involvement with each platform category. This does not establish that platform use caused victimization, that any specific platform is solely responsible for harassment, or that non-victims on these platforms face equivalent risk. The associations reflect self-

reported platform involvement among a small, non-probability sample and should be interpreted as hypothesis-generating evidence rather than definitive causal conclusions.

The near-universal skepticism about safety protocol adequacy (72.7%) is significant for the information systems community. It suggests that users broadly distrust existing governance frameworks, consistent with Citron's (2023) argument that current legal and platform-level protections are fragmented. This skepticism, shared equally by victims and non-victims, indicates that inadequate digital safety protections are a widely perceived problem, not merely a concern of those with direct victimization experience.

Limitations include the small analysis subsample (n = 44), which constrains statistical power and generalizability; the cross-sectional design, which prevents causal inference; self-report bias; and the non-probability sample, which limits representativeness. For information systems educators and practitioners, these findings suggest that digital safety literacy, platform-specific risk awareness, and victim-centered system design should be integrated into information systems curricula as core competencies.

REFERENCES

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753-1820.

Citron, D. K. (2023). Empowering speech by moderating it. Dædalus, 152(3).

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users. Cyberpsychology, Behavior, and Social Networking, 17(2), 61-67.

Fissel, E. R., Reyns, B. W., Nobles, M. R., Fisher, B. S., & Fox, K. A. (2024). Cyberstalking victims' experiences with fear versus other emotional responses. Crime & Delinquency, 70(4), 1116-1147.

Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

IBM. (2024). SPSS Statistics. https://www.ibm.com/products/spss-statistics

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. Technological Forecasting and Social Change, 163, 1-15.

Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016). Online harassment, digital abuse, and cyberstalking in America. Data & Society Research Institute.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114-133.

McHugh, M. L. (2013). The chi-square test of independence. Biochemia Medica, 23(2), 143-149.

McLuhan, M. (1964). Understanding media: The extensions of man (2nd ed.). McGraw-Hill.

Navarro, J. N., & Jasinski, J. L. (2012). Why girls? Using routine activities theory to predict cyberstalking victimization among college women. Violence and Victims, 27(5), 788-802.

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization. Justice Quarterly, 31(6), 986-1014.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. Criminal Justice and Behavior, 38(11), 1149-1169.

Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. Cyberpsychology, Behavior, and Social Networking, 24(6), 367-376.

Weekes, C. J., Storey, J. E., & Pina, A. (2025). Cyberstalking perpetrators and their methods: A systematic literature review. Trauma, Violence, & Abuse. https://doi.org/10.1177/15248380251333411

APPENDIX A: SURVEY INSTRUMENT

Survey Instructions: Cyberstalking, Digital Harassment, and Tracking Technologies

Thank you for participating in this study. This survey includes multiple-choice and short-answer questions regarding your experiences with cyberstalking, digital harassment, and tracking in online platforms and gaming environments. Your responses are anonymous and used exclusively for academic research. You may skip any question that causes discomfort. A list of support services is provided on the exit page.

For the purpose of this study, cyberstalking and digital harassment may be used interchangeably and are defined as the intentional use of any interactive computer service or electronic communication service (i.e., social media, websites, messaging applications, GPS and location trackers, spyware and stalkerware) to conduct activity that places a person "in reasonable fear" of death or serious bodily injury, or that causes or could cause "substantial emotional distress" (Federal Bureau of Investigation, 2018).

Demographic Questions

Q1. I have read and understand the information above. I am at least 18 years old. By selecting agree below, I agree to the terms and procedures of this study and agree to participate in the study. By selecting disagree I am choosing not to complete the survey and the survey will terminate. [Researcher, advisor, and IRB contact information removed for blind review.] (Agree / Disagree)
Q2. What is your age? (18 to 24 / 25 to 34 / 35 to 44 / 45 to 54 / 55 to 60 / 65 to 74 / 75 or older)
Q3. What is your gender identity? (Woman / Man / Non-Binary / Not specified above, please specify)
Q4. What is your ethnicity? Please select all that apply. (American Indian or Alaskan Native / Asian or Pacific Islander / Black or African American / Hispanic, Latino/a, or of Spanish origin / White or Caucasian / Prefer not to answer / Other, please specify)
Q5. What is your highest level of education? (Did not attend school / 1st grade through 11th grade, listed individually / Graduated from high school / 1 year of college / 2 years of college / 3 years of college / Graduated from college / Some graduate school / Completed graduate school)
Q6. What is your state of residence? (United States only; dropdown menu of all U.S. states, the District of Columbia, and U.S. territories)

Section 1: Cyberstalking and Digital Harassment

Q7. Have you personally experienced persistent, unsolicited digital communication (e.g., messages, emails, social media interactions) that caused emotional distress or concern for your safety? (Yes / No)
Q8. Platform experienced harassment? Frequency (Daily / Weekly / Monthly / Semi-Annual or Annual) for each of the following: Facebook, Instagram, TikTok, Twitter/X, Reddit, Email, SMS/Text, WhatsApp/Snapchat, Anonymous platforms, Discord, Twitch, Xbox Live, PlayStation Network, Steam, Mobile Games, Other.
Q9. Did the incident(s) include manipulated or synthetic media (e.g., deepfakes, photoshopped images, voice cloning)? (Yes / No)
Q10. Have you ever experienced unwanted digital tracking or surveillance? (Yes / No)
Q11. What type of location-based technologies (e.g., GPS metadata, IP tracking, geofencing) were used to monitor you? Select all that apply. (GPS: precise tracking systems via phones, cars, and wearable trackers / Bluetooth: short range, indoor tracking / Metadata or Geotags: social media surveillance of location / Application Activity Logs: fitness trackers or Google Maps recording travel or running routes / Messaging Apps: WhatsApp or iMessage sharing live location / Other, please specify)
Q12. Were you ever doxxed (i.e., had your personal information shared publicly without your consent) on digital platforms? (Yes / No)
Q13. What action did you take in response to the harassment and/or tracking? Select all that apply. (None of the above / Blocked user(s) / Reported to moderators or support staff / Changed username or gaming ID / Limited game access or chat participation / Ceased platform use / Reported to law enforcement / Took no action / Other, please specify)

Q14. To what extent did you experience the following emotional responses related to the incident(s)? (1 = No Emotional Response, 5 = High Emotional Response) Items: Anxiety / Fear / Anger / Depression / Distrust of digital technology
Q15. Based on your emotional response: did you seek out any form of support following the incident (mental health and emotional support services, online community groups, organizations, help lines, etc.)? (Yes / No)
Q16. Do you believe that existing safety protocols adequately address cyberstalking and digital harassment (overall)? (Yes / No)