Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

The Cost of Over-sharing: How Daily Facebook Posting Compromises Personal and Digital Security

Sharif Ratul Hassan

Undergraduate Student, Department of English, Northern University Bangladesh
hassan_47240101221@nub.ac.bd
https://orcid.org/0009-0009-8338-9595

Abstract

This study explores the risks associated with posting often on Facebook and exposes the security threat posed by the use of smart phones in making one's life vulnerable. By applying architectural and criminological theories such as Routine Activity Theory and Context Collapse, this paper explores how nine specific threat vectors have been created. It is observed that the creation of large sets of daily activity information, check ins, and high-definition media allows determined perpetrators to develop predictive behavior algorithms that facilitate generative AI deep fake extortion, home burglary, and economic fraud. Additionally, using context collapse through platforms means that the overshares by individuals reduce their social boundaries and end up negotiating away the security space for the entirety of the social network. The response to these structural threats requires an urgent change in behavior by learning to disengage from intimate sharing and implementing stringent security measures.

Keywords: Context Collapse, Deepfake Extortion, Digital Hygiene, Facebook Oversharing, Open Source Intelligence (OSINT), Routine Activity Theory, Social Engineering, Surface Area of Exposure.

1. Introduction

Social media sites have become much more integrated into people's interactions in today's digital environment. In this context, it is necessary to consider that Facebook represents the most dominant of all such social networks, uniting about 3.07 billion active monthly users and 2.11 billion daily active users in a unified network (DataReportal, 2025). As such, the use of Facebook implies the centralization of 37% of the total world's population on one platform, making the site into a global database of behavioral information. On the other hand, the changes that occur on the socio-cultural level motivate people to provide live updates, while the awareness of risks involved is not as developed. Consequently, people have acquired an unhelpful broadcasting structure: although sharing information through their accounts as part of an "illusion of intimacy" based on the assumption of interacting exclusively with friends, this

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

behavior makes people's data available for Open Source Intelligence analysis (Humphreys, 2018).

The security challenge stems from the underlying algorithmic design of the social media platform, where posting frequency and expression are rewarded. Constant sharing of everyday experiences, work-related activities, and HD media content creates predictable behavioral patterns. From the criminological perspective of Routine Activity Theory (RAT), the spatial barriers that formerly separated criminals and victims dissolve in digital environments, bringing the gap in tactics to nothing (Leukfeldt & Yar, 2016). The urge to share one's achievements as part of the "bragging culture" of contemporary consumerism encourages the practice of luxury profiling and geotagging, thereby transmitting threatening information about one's finances and time away from home (Srinivasan, 2019; W. Reyns, 2019). As a result, the personal smartphone gradually evolves into an encryption-free intelligence device designed to assist adversaries with their surveillance operations.

Moreover, the threat environment has become highly serious because of the quick spread of democracies surrounding generative artificial intelligence systems and social media platforms' social leveling. The constant production of HD selfies and videos gives the criminals everything they need for performing media manipulation or deepfake extortion schemes (Westerlund, 2019). Such vulnerabilities do not limit themselves to an individual but are also facilitated by something called "context collapse", a process that occurs as the design of social media sites collapses various separate social circles like family, classmates, or professional colleagues into one big audience (Marwick & Boyd, 2014). Once the user starts tagging the family, sharing information about parents, or checking-in at a child's school, they create a serious threat to everyone around them by exposing the privacy of the entire close-knit community to which they belong (J. Borkovich & Breese, 2016). In this paper, the author will look at the nine most significant threats associated with Facebook oversharing behavior.

2. Background and Related Works

Due to the rapid growth of social media, individual revelations have become easy targets of open-source data exploitation. This chapter analyzes the existing literature on digital surveillance, adversarial AI, and the socio-technical risks exposing frequent users to danger from both real-world and online environments.

A. **OSINT Harvesting and Algorithmic Surveillance:** Previous studies have shown that OSINT collection has changed from passive monitoring to automated and scripted processing (Humphreys, 2018). Cybercriminals no longer need any elaborate network hacks in order to identify the patterns of their target's everyday life. On the contrary, automated scrapers are used by malicious agents in order to harvest chronology logs from social media accounts. It is only necessary to analyze timestamped information, along with text and metadata, over a period of 30 to 90 days in order to produce an accurate depiction of geographic patterns and schedules on a week-to-week basis.

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

B. Generative AI and Weaponized Media: The cybersecurity threat space has seen a huge paradigm shift because of the democratization of GANs and deepfake creation methods (Westerlund, 2019). The high-definition multimedia environment of social media acts as an extensive dataset for training purposes for malicious parties. Users unknowingly contribute biometric data by uploading high-definition selfies and videos regularly; criminals use facial attributes from such images and superimpose them on videos, resulting in unauthorized deepfakes that are then used for blackmailing victims.

C. Context Collapse and Relational Vulnerabilities: An important issue of socio-technical nature in social networking design is the occurrence of "context collapse." In context collapse, different social contexts, including academia, domestic, and workplace social groups, all become a single, undifferentiated social group (Marwick & Boyd, 2014). In social networking site design, all the boundaries of these contexts get completely erased. When a user shares relational data by tagging family members or logging into their school on their account, they effectively give up their social perimeter security (J. Borkovich & Breese, 2016). In case the attacker faces strong perimeter protection for a main target, then he/she turns to secondary targets having more social connectivity within the social mapping of the user.

D. Criminological Frameworks in Cyber Environments: How digital practices lead to victimization is best measured by applying Routine Activity Theory (RAT), which states that in order for a crime to be committed, three elements have to coincide; an offender who is motivated, a target that is appropriate and a lack of an able guardian. Contemporary forms of Routine Activity Theory state that frequent social media use transforms these spatial elements such that the spatial element becomes irrelevant (Leukfeldt & Yar, 2016).

Cyber Convergence = {Motivated Offender + High-Exposure Target – Digital Guardianship}

Under the influence of contemporary consumerism, people indulge in luxury profiling, whereby PII is shared, thus making regular accounts valuable targets (Srinivasan, 2019). On the other hand, instant location tagging meets all the criteria of Rational Choice Theory in relation to property offending (W. Reyns, 2019). Through the use of instant geotagging outside one's home, users are clearly communicating that they are not at home. This provides offenders with the opportunity for conducting burglaries when the homes are unoccupied.

E. Key Research Gap: Although many studies on cybersecurity already discuss enterprise infrastructure security and classic endpoint security, there still lies a gap in exploring how the everyday behavior of consumers, their language, and even the social architecture created by certain platforms contribute to the development of extortion through artificial intelligence. In this study, the author will explore the nine key threat vectors associated with daily timeline updates.

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

3. Methodological Framework and Procedures

This study employs a qualitative socio-technical research approach based on analysis in order to investigate the ways in which everyday behavior and system features combine to produce personal and digital security risks. Rather than counting breaches, this approach considers behavior alongside recognized cyber security and criminal threat frameworks.

A. **Data Source and Selection Strategy:** The entire process utilizes OSINT intelligence and secondary data from multiple platforms. The data collection involves a data set composed of publicly available network meta data, industry cyber security reports (2024 – 2026), and behavioral timelines. A purposive sampling methodology was used to identify cases wherein the behavioral data resulted in either a cyber-attack or a physical attack. Data collection was completely passive in nature and all identifiable PII was stripped of any form of identification.

B. **Analytical Frameworks:** The gathered qualitative data is interpreted through a multi-dimensional framework:

- **Routine Activity Theory (RAT):** Analytical method used in assessing how digital activities alter traditional spatial parameters, bringing the space that exists between an attacker and the victim to zero.
- **Context Collapse Paradigms:** Tools used in understanding how flat social media designs make users trade off the group-level security of their relational networks.
- **The Cyber Kill Chain (Reconnaissance Phase):** Model used in identifying how unstructured timeline footprints can be scraped and analyzed for use by attackers.

C. **Procedural Pipeline:** The execution of the study follows three distinct procedural phases:

Data Acquisition	Phase 1	Extracting open-source behavioral traits, luxury profiling patterns, and geotagging frequencies from public data repositories and platform case studies.
Thematic Categorization	Phase 2	Coding and grouping the gathered behaviors into the nine distinct risk boundaries (e.g., algorithmic routine analysis, generative deepfake vulnerability, geospatial disclosure).
Threat Vector Mapping	Phase 3	Aligning each categorized behavior with its corresponding physical or technical weaponization mechanism (such

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

		as GAN training, SIM-swapping infrastructure, or vacant home burglary).

D. **Methodological Boundaries:** These tactics are subject to certain constraints. First, they function only through the use of publicly accessible computer infrastructure, in that they do not examine any data flows occurring within privately secured end-to-end encrypted messenger networks. Second, since generative artificial intelligence technology and automated adversarial scraping scripts advance quickly, this set of threats reflects an ongoing baseline for future consideration.

4. Analysis and Findings

A. Demographic Macro-Analysis and the Surface Area of Exposure

For a scientific analysis of the impact that everyday activity on Facebook has on one's privacy, it becomes essential to first analyze the structural attributes and demographics of Facebook. At present, Facebook stands as a digital storage center that holds about 3.07 billion MAUs and 2.11 billion DAUs (DataReportal, 2025). With this much presence, almost 37% of the total world population is consolidated into one architecture, which makes Facebook a huge repository of information that can be misused. Globally, the gender split is 56.8% males and 43.2% females (statista, 2025). Although there are more males in numbers, the gender inequality in cyber-criminality is that women have a much higher chance of non-consensual media manipulation and being victims of cyber-blackmailing than men, who have a higher chance of socio-economic fraud and identity theft. The core behavioral driver behind the security crisis is uncovered when isolating the age demography of the platform:

Age Cohort	Global User Share (%)	Primary Vulnerability Indicator
18–24 years	18.6%	High Multimedia Saturation & Ephemeral Intimacy Risk
25–34 years	24.97%	Socio-Economic Signaling & Routine Predictability
35–44 years	18.68%	Generational Network Mapping & Familial Exposure
45–54 years	14.2%	Low Digital Hygiene & High Phishing Susceptibility

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

55–64 years	11.7%	High Cognitive Vulnerability to Financial Scams
65+ years	6.1%	Institutional Social Engineering Targets

The demographic age range between 25-34 years (24.97%) along with age group 18-24 years (18.6%) constitute about half of the total world population of users. Being university students or young professionals, they are active participants spending 33-34 minutes each day posting and commenting on the site (statista, 2025). This amounts to over 17 hours of encrypted broadcasting each month. The continuous flow of data generated from such activity provides attackers the necessary data to commit both physical and cybercrimes against the individual.

B. Comprehensive Evaluation of the Nine Major Threat Vectors

- **Algorithmic Routine Analysis and Pattern Recognition:** A pattern that emerges when a Facebook user is updating their profile several times a day, is the construction of a very predictable behavioral map. Regular logging into Facebook, posting complaints about daily traffic, or adding pictures from a daily workplace becomes an OSINT scraping job by the adversary (Humphreys, 2018). Attackers who gather timestamps, metadata of pictures, and other textual information over a span of 30 to 90 days can develop an accurate chronology of the victim's whereabouts. The use of pattern recognition software can then ascertain with high statistical reliability where the target is going to be at any time throughout the week. This obviates the necessity of conducting surveillance for the criminals. Oversharing essentially makes it easy for the stalker or kidnapper by automating surveillance prior to an attack.
- **AI-Driven Media Manipulation, Generative Deepfakes, and Digital Extortion:** Fast development in Generative Artificial Intelligence (AI) and Generative Adversarial Networks (GANs) has drastically transformed the threat environment in relation to multimedia sharing. Individuals uploading their daily selfies, family photos, or videos are unwittingly contributing to a formidable training data set for the wrong people. The cyber criminals exploit these open sources to process the data through an AI application to generate non-consensual media, popularly known as deepfakes (Westerlund, 2019). In the deepfake creation process, the algorithm transfers facial features of the targeted victim on pornographic or compromising videos. These artificially generated files act as tools of extortion to psychologically abuse and extort victims by blackmailing them. The blackmailers approach the victims and threaten them with broadcasting the deepfake on their work environment, academic institutions, or social networks.
- **Inbox Vulnerabilities, Ephemeral Intimacy, and Interpersonal Breaches:** The Facebook Messenger environment is typically seen as a safe haven of encryption and privacy by users, resulting in the emergence of "ephemeral intimacy," wherein people share private, sensitive,

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

and intimate information through Facebook Messenger. Nevertheless, empirical results show that the Facebook Messenger inbox is amongst the most unstable data storage sites owing to the presence of two forms of attacks. To begin with, any breach of security either through phishing attacks or session hijacking allows the attacker to instantly access the complete database of past chat history. The chat history is scrutinized for any kind of confidential media, company documents, or personal confessions which are later exploited through blackmailing. Secondly, when there occurs any breakdown in a relationship either on a professional level or romantically, this results in revenge leakage where intimate chats or media files are leaked in public to defame the individual.

- **Geospatial Context Collapse via Instantaneous Check-Ins:** Real-time geotagging is a breach of perimeter security. Once a consumer opts to check-in at an upscale restaurant, a vacation destination, or an airport instantly, they are sharing two separate sets of information with the world around them, one being their exact location while the other being their location away from home. From the point of view of criminology, this falls squarely into the "Rational Choice Theory" model of modern burglary (W. Reyns, 2019). Criminal organizations regularly track localized hashtags and live check-ins in order to locate valuable properties which are sure to be empty. By posting a check-in at the airport, accompanied by a caption such as "Going to Bangkok for two weeks!", the user offers the burglars a timeframe in which to commit a break-in.
- **Network Mapping and Close-Circle Exposure:** The architecture of Facebook makes it easy for individuals to construct a socio-demographic map that shows their family relations, friends, and romantic relationships. Although this activity aims to bring people closer, in reality, it exposes the individual's "Close Circle" to the adversary's surveillance in a phenomenon known as "Context Collapse" (Marwick & Boyd, 2014). If the perpetrator chooses a particular target but finds that their defenses are too strong, then he or she can simply focus on targeting other people who are tagged by the potential victim. For example, a video taken of a child's first day at school by tagging the school's page means that the criminal knows the daily physical schedule of the child. Such details are often used for virtual kidnappings where fraudsters call the child's parents, threaten them with kidnapping, and request a direct online bank transfer.
- **PII Harvesting, SIM-Swapping, and Social Engineering Infrastructure:** Facebook posts made daily tend to inadvertently reveal Personally Identifiable Information such as phone numbers, emails, and employment details. The perpetrators make use of automated scraping scripts to gather such information, which they then use to profile the target individual and conduct social engineering attacks (Jagatic et al., 2007). The most obvious risk arises if the compromised phone number is targeted through a SIM swap scam. Using the information available from a timeline in PII (birthdays, names of the victim's parents, or places where they have been), hackers will trick mobile carriers into switching the number to another SIM controlled by the hackers, thereby gaining access to 2FA and OTPs. This allows for full entry into financial sites, primary email, and even business networks.

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

- **Socio-Economic Signaling and Luxury Profiling:** This modern socio-cultural shift into digital consumerism has resulted in the emergence of a "bragging culture." Users tend to flaunt their luxury purchases, costly devices, fancy cars, and lavish lifestyle elements. This behavior trend is referred to as "Luxury Profiling" in modern cyber security terms (Srinivasan, 2019). The act of showcasing the presence of financial resources will immediately make such users be classified as “High-Value Targets” (HVT). Online scammers, ransomware distributors, and extortioners will target these profiles more than other ordinary profiles since the expected ROI from hacking an HVT profile is greater than from other accounts.
- **Interactive Social Intelligence Gathering and Gamified Scams:** One of the vectors that can be easily deceiving in a user's everyday use of Facebook is their participation in games, third-party quizzes, and trends (for example, "See what your future house looks like" or "Who among your friends loves you the most?"). In order to take part in such activities, users have to go through the Facebook interface that requests the user to provide API access to any third-party developer (Al-Saggaf & Islam, 2014). Most often, these apps are a front for data mining for criminal activities. These permissions give access to friend lists, email addresses that may not be made public, and personal timelines. Moreover, the quiz questions themselves can be designed in such a way that they get responses that could be used to bypass account security measures by asking the names of your pets, favorite teachers, and street names in which you grew up.
- **Digital Footprint Aggregation and Corporate or Adversarial Surveillance:** Each post, reaction, share, and comment leaves behind a digital footprint that cannot be changed. As the user is concerned with their immediate actions, the big picture for the data brokers and others who are adversarial will come from an analysis of the data collected over a long period of time. Such data are extremely prone to corporate espionage and malicious use. For instance, if a particular user’s digital footprint indicates certain political views, emotional weaknesses, or triggers, cyber criminals will be able to launch a disinformation campaign or phishing scam that specifically targets their psychological state. Thus, it transforms an ordinary security issue into an elaborate form of psychological manipulation.

5. Discussions and Critical Evaluation

The results collected from the nine major attack vectors make a disturbing discovery about the current dynamics in social media usage. There exists a serious structural inequality between users' intentions and capabilities of the adversary. For instance, when the users interact on Facebook, they do so in the "illusion of intimacy" as defined by cyber psychologists. This means that they believe their timelines to be a safe haven occupied only by positive people.

By way of direct contrast, however, the threat actors perceive these very same open or semi-open information feeds as being repositories of unsecured intelligence. As physical surveillance gives way to automated surveillance, the user need no longer be stalked in order to be victimized. Rather, the constant production of high-definition imagery, real-time location data, and relation tagging enables the petty criminal to conduct highly complex operations utilizing OSINT and generative AI tools. This vulnerability in behavior is embedded in the nature of the structure of

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

the platform. The algorithms of Facebook have been built with the aim to encourage frequent posts along with emotional content, leading to a blending of all social boundaries. In real life, one keeps clear distinctions between different social environments. One behaves differently among university lecturers than among family and friends.

Context collapse is what happens here in its entirety, a term that has been used within the study of communication to refer to the same (J. Borkovich & Breese, 2016; Szabla & Blommaert, 2018). When one posts information on the status such as location, tagging a romantic relationship or indulging oneself in a luxurious purchase, then this is shared to an amorphous audience that lacks distinctions. Relational privacy requires that security be something collective rather than personal. Through posting information about the family member or even tagging a child's school, the main user ends up negotiating their perimeter security.

The fast democratization of generative AI tools, especially Generative Adversarial Networks (GANs), means that the routine task of sharing personal media is now weaponized. Previously, deepfake extortion or sophisticated identity fraud was only achievable by individuals with sophisticated cyber-capabilities or who allocated a lot of resources. Now, the amount of multimedia data produced ensures there are sufficient training sets.

From the demographic perspective, individuals aged 18-34 comprise almost half of the platform users, spending over 17 hours per month live-broadcasting their lives. Under the lens of Routine Activity Theory in Criminology (RAT), online settings change the conventional spatial variables involved in a crime, since the distance between the perpetrator and the target becomes equal to zero (Leukfeldt & Yar, 2016). Online routines allow motivated criminals to be more visible on social media platforms and overcome barriers without being detected by conventional user guardianship (Ahmad & Thurasamy, 2022). Such an audience is easily exploitable in terms of online extortions and predictive physical stalking. Thus, the results indicate that everyday routine of live-posting on Facebook has turned one's smartphone into a broadcast source which poses threats to the individual's physical safety, financial stability, and overall wellbeing despite its socializing role.

A. Threat Vector Matrix: The following table provides a structural synthesis of the findings, mapping each specific Facebook activity to its corresponding technical or physical threat mechanism and primary safety outcome:

User Activity or Behavior	Technical or Physical Mechanism	Primary Security Outcome
High-Frequency Posting & Daily Updates	Open Source Intelligence (OSINT) scraping and algorithmic pattern recognition over a 30 to 90-day span.	**Predictive Stalking:** Automates pre-operational physical surveillance and eliminates the need for physical tracking.
Uploading HD Selfies, Photos, & Videos	Data extraction via Generative Adversarial Networks (GANs) and	**Deepfake Extortion:** Production of non-consensual altered explicit

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

	generative AI synthesis software.	media used for financial and psychological blackmail.
Staging Sensitive Media & Chats in Inbox	Credential harvesting, session hijacking, and unauthorized screenshot preservation.	**Intimate Data Leaks:** Exposure of private archives during account compromise or interpersonal relationship dissolution.
Real-Time Geotagging & Check-Ins	Broad-spectrum broadcasting of live spatial coordinates, aligning with Rational Choice Theory.	**Vacant Home Burglary:** Signaling physical absence from a primary residence, creating risk-free windows for break-ins.
Tagging Family, Friends, & Partners	Multi-dimensional network mapping and systemic data aggregation across flattened social circles.	**Virtual Kidnapping:** Exploitation of family routines and school data to execute highly authentic, fraudulent extortion scams.
Exposing Public Email, Phone No, & Work	Automated scraping scripts targeting public Personally Identifiable Information (PII).	**SIM-Swapping & Phishing:** Interception of Two-Factor Authentication (2FA) codes to bypass banking and primary account security.
Displaying Luxury Purchases & Lifestyle	Socio-economic profiling and financial targeting of perceived wealthy accounts.	**High-Value Target Profiling:** Elevated frequency of hyper-targeted spear-phishing and localized extortion operations.
Participating in Third-Party Quizzes or Trends	Arbitrary blanket API access permissions granted to unverified malicious external applications.	**Social Intelligence Harvesting:** Extraction of private datasets and answers used to bypass account security questions.
Accumulating Continuous Timeline	Longitudinal digital footprint aggregation and automated psychological profiling by	**Cognitive Manipulation:** Deployment of micro-targeted disinformation

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

History	data brokers.	campaigns and weaponized social engineering scams.

6. Strategic Implications for the Individual User

The inevitable result of constant Facebook usage and posts is the gradual erosion of the individual's sovereignty. On an individual level, it means that it will no longer be possible for the individual to keep going along with his or her habitual online behavior. By using his or her social media account as a virtual diary, the individual inadvertently gives an outline of all activities he or she performs in the course of a day. This is because today's social media platforms have to be seen as public broadcasting venues rather than private social networking spaces.

[Old User Mindset]	**[Required Security Mindset]**
Profile as a Private Diary	Profile as a Public Broadcast
• Reactive to privacy alerts • Post first, consider risks later • High emotional expression	• Proactive content filtering • Immediate risk assessment per post • Strategic information containment

7. Limitations of the Study

The methodology of this study is limited by multiple parameters, which affect the breadth of the study. First, it should be noted that the research is purely qualitative, using well-known models from architecture and criminology instead of actual quantitative data on the frequency of security breaches. Secondly, since the study utilizes metadata across the entire world, the individual experiences of certain social strata, specific to certain regions, are not taken into account. Finally, since the methods used in generative artificial intelligence, and data scraping technologies progress exponentially, cybercrime tactics may change much faster than defense mechanisms and academic literature.

8. Conclusion

To sum up, excessive posts on Facebook cause a very serious security crisis because they transform private cell phones into intelligence sources of an open code for any malicious parties involved. Daily updates, check-ins, and photos in high definition make physical tracking redundant, as they allow the automation of the whole process of blackmailing victims using deepfakes, burglarizing empty apartments, and conducting highly targeted financial fraud. Owing to the fact that the system architecture itself leads to the total breakdown of context, each individual becomes a threat to all other members of his or her social network, as well as to its safety zone.

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

References

[1] Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. *Journal of Cyber Security and Mobility*, *11*(3). https://doi.org/10.13052/jcsm2245-1439.1133

[2] Al-Saggaf, Y., & Islam, M. Z. (2014). Data Mining and Privacy of Social Network Sites' Users: Implications of the Data Mining Problem. *Science and Engineering Ethics*, *21*(4), 941–966. https://doi.org/10.1007/s11948-014-9564-6

[3] DataReportal. (2025, July). *Global Social Media Statistics*. DataReportal – Global Digital Insights. https://datareportal.com/social-media-users

[4] Humphreys, L. (2018). *QUALIFIED SELF : social media and the accounting of everyday life.* Mit Press.

[5] J. Borkovich, D., & Breese, J. (2016). SOCIAL MEDIA IMPLOSION: CONTEXT COLLAPSE! *Issues in Information Systems*, *17*(4), 167–177. https://doi.org/10.48009/4_iis_2016_167-177

[6] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

[7] Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: a Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

[8] Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://journals.sagepub.com/doi/10.1177/1461444814543995

[9] Srinivasan, R. (2019). *Whose global village? : rethinking how technology shapes our world*. New York, New York University Press.

[10] statista. (2025). *Topic: Facebook*. Statista. https://www.statista.com/topics/751/facebook/?srsltid=AfmBOooAULlSfDx2ocsx02ECARiNLVB3Mihit4iOjaiYaUVs1XeDgF_C#topicOverview

[11] Szabla, M., & Blommaert, J. (2018). Does context really collapse in social media interaction? *Applied Linguistics Review*, *0*(0). https://doi.org/10.1515/applirev-2017-0119

Received: 2026-03-31
Accepted: 2026-06-14
Published Online: 2026-06-20
DOI: 10.70454/IJMRE.060203

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[12] W. Reyns, B. (2019). Online routine activities and digital victimisation: Assessing the factors that increase cybercrime vulnerability. *Journal of Criminology*, *52*(2), 201–218. https://doi.org/10.1177/0022427818811462

[13] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, *9*(11), 39–52. https://timreview.ca/article/1282