An Impact on Privacy, Safety and Security Concerns in the Age of Social Media

[1]Vivek Gupta, [2]Sindhu P, [2]Shubham Chaudhary, [2]Saksham Kothari, [2]Shrusthi Ijmulwar, [2]Aditya Sharma, [2]Mohit Sonigera

[1]Assistant Professor JU-CMS,Bangalore.[2]Student at JU-CMS.

ABSTRACT

This article explores the diversity of privacy and security in the context of social media platforms. As society increasingly relies on these platforms for communication, networking and information sharing, the risks associated with privacy breaches and data security holes have become more prominent. This study draws on the extensive existing literature and examines various dimensions of privacy violation, including data collection, surveillance practices, and algorithmic manipulation. In addition, it examines the shortcomings of current regulatory frameworks and industry practices to protect user privacy and ensure data security.Using case studies and empirical analysis, the article explores the real impact of privacy breaches and data security breaches on individuals, organizations and society as a whole. Finally, it proposes a comprehensive approach to address these issues and emphasizes the need for improved user education, technical innovation and regulatory measures to promote a safer and more private online environment.

Keywords:Data Breach,Privacy Concerns,Cyber Security,Transparency,Privacy Violations

INTRODUCTION

With a rise in the number of internet users in recent years there has been a significant rise in the number of social media users as well. While this is a favorable outcome of a more technologically equipped generation it also generates multiple issues related to social media security such as privacy and safety concerns and it is also laborious to handle such issues due the dimension of the users and up to the minute methods or approach of cyber fraudsters,hackers etc.Privacy is a fundamental right of every individual and cannot be compromised with upgradation of technology and growing risk of misusing data.While this data is available to anyone who is granted access with due procedure, one cannot assure how a potential cyberpunk may wish to misuse it and it becomes a challenging task to detect the actual offender and in most cases the offender might remain on loose and cause additional trouble to the users.Hence users need to take possible precautions and measures to prevent such an adverse situation from affecting them as the effect might lead to dangerous outcome and can cause harm or injury to the user.Depending upon the data provided by the users, the data at risk may consist of Health Information,Shared Location ,Personal photos and messages,Family details,Sexual Orientation,Religious Identity, and much more information.

While most users believe altering privacy settings according to their preferences continues to keep their data safe this might not be the reality as data published on the internet once is at high risk and not completely safe as one may believe regardless of the privacy settings.

Social media platforms can gather private information and users' private data, including health care or health records, biometric info, educational institutions records, credit card data, financial data, personal identifiers like age, ethnicity, and race, photos of users' faces, information from job applications and status updates, life and relationship incidents, religious beliefs, content shared on social media, and participation on social networking sites.

Due to the large amount of confidential data we post on social media, privacy is extremely important in this environment. Information about our lives, connections, interests, and even where we are may be found on our social media pages. This abundance of personal data is susceptible to misuse, data breaches, identity theft, and unauthorized surveillance without the right privacy controls.For the sake of preserving our individual autonomy, defending our digital identities, and ensuring authority over our personal information, maintaining privacy on social media is essential. By putting privacy first, we can encourage trust and confidence in the digital world, enabling people to interact and express themselves freely without risking their personal security.The advent of social media platforms has undeniably transformed the way we connect, communicate, and share information. These digital ecosystems have woven themselves into the fabric of our daily lives, offering unprecedented opportunities for global interaction, content dissemination, and personal expression.The rise of social media has ushered in an era of unparalleled interconnectedness, allowing individuals to bridge geographical gaps and engage in conversations across cultures, languages, and time zones. Platforms like Facebook, Twitter, Instagram, and TikTok have become integral to how we build relationships, stay informed, express our identities, and participate in public discourse. However, this unprecedented connectivity has also exposed us to a range of vulnerabilities, necessitating a nuanced understanding of the risks involved.One of the foremost concerns in this digital landscape is privacy. As users willingly share personal information, thoughts, and experiences online, questions about the extent to which our data is collected, processed, and monetized by social media companies have become increasingly pertinent. The Cambridge Analytica scandal, among others, shed light on the intricate web of data harvesting and the potential for manipulation, raising profound questions about user consent, data ownership, and the protection of personal information.Simultaneously, the safety of individuals in online spaces has emerged as a critical concern. Social media has become a platform for cyberbullying, harassment, hate speech, and the spread of misinformation. The consequences of these negative interactions can be severe, affecting mental health, reputation, and even physical safety. Consequently, safeguarding users from such harm has become a complex challenge, necessitating a balance between free expression and responsible moderation.

Security, too, is a paramount issue. Social media platforms have been targeted by malicious actors seeking to compromise user accounts, disseminate malware, or engage in disinformation campaigns. These security breaches can have far-reaching consequences, not only for individuals but also for the integrity of democratic processes and the stability of societies.This research endeavors to delve into these pressing concerns, examining the evolving landscape of privacy, safety, and security in the age of social media. It seeks to dissect the intricate relationships between technological advancements, user behaviors, and the policies and regulations that govern these digital spaces. By doing so, it aims to provide insights into potential solutions, best practices, and the ethical considerations necessary to strike a balance between the benefits and risks associated with social media use in the 21st century.

OBJECTIVES AND SCOPE OF THE STUDY

One of the primary objectives is to comprehend how users interact with social media platforms concerning privacy, safety, and security. This includes studying user practices, preferences, and the factors influencing their decisions.

Identify the vulnerabilities and weaknesses within social media platforms and user behaviors that can lead to privacy breaches, safety threats, and security incidents.

Develop strategies and recommendations to mitigate privacy, safety, and security risks on social media, including technological, policy, and educational interventions.

Analyze the impact of existing privacy and security regulations (e.g., GDPR, CCPA) on social media platforms and their users, and propose enhancements or alternative regulatory approaches.Stay current with evolving threats such as deep fakes, AI-driven cyberattacks, and new social media platforms to proactively address emerging challenges.

Develop specific strategies to protect vulnerable groups, including children, teenagers, and marginalized communities, from privacy, safety, and security threats.

Encourage ethical practices among social media companies, including transparent data handling, responsible content moderation, and accountable data sharing practices.

Investigate how social media platforms collect, store, and share user data, and assess the implications of data privacy policies and user consent mechanisms.

Examine the prevalence and impact of cyberbullying, online harassment, and harmful content on social media, and propose methods to enhance user safety.

Assess the security measures employed by social media platforms to protect user accounts and sensitive information, and explore potential vulnerabilities.

Study user behavior patterns related to privacy settings, sharing habits, and security practices on social media.Analyze the legal and regulatory landscape governing social media and how it impacts user rights, platform responsibilities, and corporate practices.

Investigate the broader societal impact of privacy, safety, and security concerns on issues such as democracy, free speech, mental health, and social cohesion.

Research and develop technological solutions to enhance privacy, safety, and security on social media platforms, including encryption, authentication, and content filtering.

.Explore the ethical dimensions of data collection, content moderation, and user engagement strategies employed by social media companies.

Consider the global nature of social media and how cultural, legal, and regional factors influence privacy, safety, and security concerns.

In summary, the objectives and scope of research on privacy, safety, and security concerns in the age of social media are wide-ranging, encompassing various aspects of user behavior, platform practices, regulatory environments, and technological innovations. The ultimate goal is to create a safer and more secure online environment for social media users while respecting their privacy rights and fostering responsible digital citizenship.

REVIEW OF LITERATURE

The study named “Social network security: Issues, challenges, threats, and solutions by (Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017))” uses a communication system that combines user-created profiles to analyze the effects of Services that connect users with their friends, family, and coworkers. These services have become very well-liked because users can update their private information, interact with other users, and view the profiles of other members.

Reviewing essay “The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks” aims to assess the risks associated with social media use because it has become more widespread recently, even among young people. Media consumption and Internet usage have rapidly increased since the start of the COVID-19 epidemic period. When teens use the Internet on their own, they primarily use YouTube, Instagram, and TikTok to access social media. Internet use allowed for peer communication and ongoing activities, such as classroom instruction, during a "lockdown". Privacy has evolved over time and now has a variety of dimensions, claim several studies (Acquisti et al., 2015; Hong and Thong, 2013; Smith et al., 2011; Westin, 2003). Mobile devices now make up about 55% of all Internet usage in the US in 2019, according to Statcounter. Personal computers dominated how people accessed the internet in recent years. Modern mobile (including wearable and embedded) devices have sensors that gather data on a range of topics, such as users' social lives (for example, time-stamped location data), sleeping patterns, and other geospatial data. In exchange for enhancing user experience and providing targeted advertisements, such information is given to mobile device manufacturers and app developers (Gal-Or, Gal-Or, & Penmetsa, 2018).

The purpose of this study was to investigate how users' perceptions of risk and their privacy concerns with regard to social media sites' collection and use of their personal information interacted. A Likert-type instrument with seven constructs was used to collect data from students enrolled in a university in the Southeast of the United States; six of the constructs described users' concerns about social media privacy, and the seventh construct described users' risk perceptions. All students (N = 138) used Facebook as their only social networking platform. Multiple regression analysis was used to analyze the data after it had been collected. The results demonstrated that subjects' perceptions of risk are influenced by three social media privacy concerns, namely collection, error, and awareness. The Findings and their implications are discussed.

Article discusses an exploratory study that looked at the relationship between computer anxiety and the Big Five personality traits as antecedents of people's concerns about their information privacy (CFIP) on social media platforms and the relationship that developed between people's CFIP and their behavioral intentions to give their personal information to online merchants. People who score highly on agreeableness and conscientiousness are worried about the privacy of their information on social media platforms, according to research using data from 298 undergraduate students. Contrary to expectations, it was discovered that computer anxiety negatively correlated with behavioral intentions. The relationship between computer anxiety and behavioral intentions was found to be fully mediated by CFIP. The discussion includes implications for theory and practice.

According to “Teens, Social Media, and Privacy” Teens divulge a lot of personal information on social media sites; In fact, the sites themselves are created to promote network growth and information sharing. However, few teenagers use social media in a completely public way. Instead, they take a variety of measures to limit and edit their profiles, and their strategies for managing their online reputations differ significantly depending on their gender and network size. The following are some of the main conclusions from a recent study that examines teens' privacy management on social media sites and is based on a survey of 802 teenagers.

A Study"Understanding and Changing Older Adults' Perceptions and Learning of Social Media" states that Despite using a variety of digital media, older people (65+) have been slower to adopt social media in particular. The potential impact of privacy concerns as a deterrent to social media adoption in this group is examined in this study. We analyze in-depth interviews with 40 older people who use and don't use social media in East York1, Toronto, Canada, to examine the different types of social media privacy concerns older adults have as well as the steps they take to allay these worries.

Given the prevalence of the exchange of personal information online, this study examines the effects of Facebook use on privacy perceptions and self-disclosure behaviors over a 5-year period from 2010 to 2015. Research from around the world supports Facebook's socializing function in promoting laxer privacy attitudes, which in turn increases self-disclosure in both offline and online settings. According to longitudinal patterns, risk perceptions increased for heavy users but remained stable for light users. Additionally, over time, there was less of a negative correlation between self-disclosure and privacy concerns. Examined are the implications of the cultivation theory in the context of contemporary social media, as well as the yearly variations in how Facebook use affects privacy attitudes and self-disclosure.

A five-year study of Facebook users' self-disclosure habits and privacy beliefs reveals that social media is helping to shape users' perceptions of privacy.

Nancy Signorielli, Mina Tsay-Vogel, and James Shanahan, New Media & Society 20 (1), 141–161, 2018.

Given the prevalence of the exchange of personal information online, this study examines the effects of Facebook use on privacy perceptions and self-disclosure behaviors over a 5-year period from 2010 to 2015. Research from around the world supports Facebook's socializing function in promoting laxer privacy attitudes, which in turn increases self-disclosure in both offline and online settings.

The role of trust and privacy concerns in COVID-19's moderating effect on social media use for e-retail services

Maram Saeed Alzaidi 68, 103042, Goma Agag, 2022 Retailing and Consumer Services Journal.The COVID-19 outbreak has had an effect on consumer shopping and buying behavior. This study utilizes social media in an effort to provide a comprehensive model of the vital roles that trust and privacy concerns play in influencing consumer purchasing behavior. It also looked at the mediation of these associations by COVID-19. Quantitative data were collected quantitatively using a survey technique through questionnaires to address various levels of the study. 600 consumers were tested prior to COVID-19, and 600 more were tested during COVID-19, for a total of 1,200 consumers. It made use of structural equation modeling with partial least squares.

The advent of social media platforms has transformed the way we communicate, share information, and connect with the world. However, this digital revolution has brought to the forefront a host of pressing concerns related to privacy, safety, and security. As we navigate this interconnected landscape, it becomes crucial to examine the multifaceted challenges and their far-reaching implications.

Privacy, once considered a fundamental human right, has come under scrutiny in the age of social media. Users willingly share vast amounts of personal information, often underestimating the consequences.Social media platforms are formidable data collectors, amassing information about users' preferences, behaviors, and interactions.

Social media has become a conduit for the rapid dissemination of misinformation and fake news. These falsehoods can fuel public health crises, affect elections, and sow discord in society. Protecting children and teenagers from online predators and inappropriate content is paramount. Users are confronted with the ethical dilemma of whether the convenience of free social media services is worth the compromise of their privacy.

Privacy, safety, and security concerns in the age of social media are complex, interconnected issues that demand immediate attention and ongoing research. Balancing the convenience and connectivity offered by social media with the protection of user rights and well-being requires a multifaceted approach. It involves user education, enhanced platform policies, ethical considerations, and technological innovations. As we continue to navigate this digital frontier, addressing these concerns is paramount to creating a safer and more secure online environment for all.

RESEARCH GAP

Research on privacy, safety, and security concerns in the age of social media has been extensive, but there are still several notable research gaps:

Longitudinal Studies: There's a need for more longitudinal studies that track how individuals' privacy attitudes and behaviors change over time as they engage with different social media platforms. This can help identify evolving trends and potential interventions.

Cultural Variations: Many studies focus on Western social media platforms and user behavior. Research should explore cultural variations in privacy and security concerns, as these can significantly differ across regions.

Algorithmic Transparency: Investigating the transparency of social media algorithms and their impact on user privacy and content dissemination is crucial. Understanding how algorithms affect the spread of misinformation and polarizing content is an ongoing concern.

User Empowerment: Research should explore ways to empower users with better privacy controls and tools. Studying the effectiveness of privacy settings and user education on social media platforms is essential.

Impact on Mental Health: While there's research on the relationship between social media use and mental health, more studies are needed to understand the nuances of this connection, including how privacy concerns might contribute to mental health issues.

Cybersecurity Threats: Investigating emerging cybersecurity threats on social media platforms, such as data breaches, phishing attacks, and identity theft, is crucial to ensure user safety.

Ethical Considerations: Research should delve into the ethical implications of data collection, user profiling, and ad targeting on social media platforms, especially in cases where user consent might be ambiguous.

User Vulnerabilities: Understanding the vulnerabilities of different user groups, such as children, elderly users, or marginalized communities, in the context of social media privacy and security is essential.

Legal and Regulatory Aspects: Research should continue to assess the effectiveness of legal frameworks and regulations in addressing privacy and security concerns on social media, as these are continuously evolving.

Privacy-Enhancing Technologies: Exploring the development and adoption of privacy-enhancing technologies, like blockchain or federated social networks, and their potential to mitigate privacy and security issues on mainstream platforms.

These gaps represent areas where ongoing research efforts can contribute to a deeper understanding of the complex issues surrounding privacy, safety, and security in the age of social media.

RESEARCH METHODOLOGY

Research methodology is the specific procedures or techniques used to identify, select, process, and analyze information about a topic.

Research Design:

* **Exploratory Research:** Given the evolving nature of social media, an exploratory approach will be employed to gain a deeper understanding of the multifaceted concerns.

* **Mixed-Methods:** A combination of quantitative and qualitative methods will be used to provide a comprehensive analysis.

* Data Collection:

* a. Surveys and Questionnaires:

* Conduct large-scale surveys to gather quantitative data on user perceptions, behaviors, and experiences related to privacy, safety, and security on social media platforms.

* Include questions on demographics, platform usage, privacy settings, and experiences with online harassment or security breaches.

* b. In-Depth Interviews:

* Conduct qualitative interviews with selected participants to delve deeper into their experiences and attitudes regarding privacy and security on social media.

* Target individuals with diverse backgrounds and experiences to capture a wide range of perspectives.

* c. Content Analysis:

* Analyze public content on social media platforms, focusing on trends in cyberbullying, misinformation, and data privacy concerns.

* Employ natural language processing techniques to identify patterns and sentiments in user-generated content.

* d. Secondary Data:

* Gather relevant data from academic studies, industry reports, and government publications to provide context and support the research findings.

* Sampling:

* Use stratified sampling techniques to ensure a representative sample of social media users from different age groups, genders, and geographical regions.

* **Data Analysis**:a. Quantitative Analysis:

* Employ statistical software to analyze survey data, including descriptive statistics, regression analysis, and hypothesis testing to identify correlations and trends.

Examine variables such as privacy settings, security breaches, and user behaviors.

* b. Qualitative Analysis: Utilize thematic analysis to identify recurring themes and patterns in interview transcripts.

Develop rich narratives to illustrate the experiences and perspectives of participants.

* c. Content Analysis: Use natural language processing tools and sentiment analysis to process and interpret the textual data from social media content.

Identify key themes, sentiment trends, and emerging issues.

* Ethical Considerations: Ensure the privacy and consent of research participants by anonymizing data and obtaining informed consent.

Adhere to ethical guidelines regarding sensitive topics such as cyberbullying and harassment.

* Triangulation: Combine findings from surveys, interviews, and content analysis to triangulate results and provide a more robust understanding of the research questions.

* Limitations :Acknowledge potential limitations such as self-reporting bias in surveys, the dynamic nature of social media, and the evolving landscape of privacy and security concerns.

* Policy and Practical Implications: Translate research findings into actionable recommendations for social media platforms, policymakers, and users to enhance privacy, safety, and security on these platforms.

* Dissemination: Share research findings through academic publications, conferences, and policy briefs to contribute to the ongoing discourse on social media concerns.

By employing this comprehensive research methodology, the study aims to shed light on the intricate dynamics of privacy, safety, and security in the age of social media while offering practical insights for addressing these critical issues.

DATA ANALYSIS AND INTERPRETATION

The survey found that adults aged 20-22 use social media often, while those aged 18-20 use it virtually daily. More than 52% of individuals are unsure whether their personal information on social media is appropriately protected, while approximately 8% are confident in the protection of their data.

When it comes to privacy and safety concerns on social media, approximately 48% of respondents are concerned. Not to mention that only 54% of the total crowd reviewed and adjusted their privacy settings on social media in the last year; the remaining 30% did not use the feature, resulting in a privacy breach on social media (e.g., unauthorized access to your account, personal information exposed).

When it comes to safety, cyberbullying is a significant issue. According to the survey, approximately 17% of respondents experienced cyberbullying as a result of a data breach, with another 16% unsure. Only 16.5% of respondents reported experiencing cyberbullying or harassment while online. Only 61% of respondents believe they will only report incidences of cyberbullying or harassment.

Only 23.1% believe it is possible to hide personal information online, while the majority of people are unsure. 33% of respondents believe that changing their account settings to 'Private' is a safer option. The majority believe that social media platforms do not do enough to protect users' privacy.

Personal information, such as sexual orientation, date of birth, location, and permissions, is truly necessary for social networking networks. In order to maintain transparency. Around 46% believe that marketers employing carbon prints or history to recommend personalized advertisements to you is a violation of your privacy. The majority of users discovered potential hackers or malware on social media. Regarding security concerns, very few people update their social networking platform passwords; a handful do so on occasion, and approximately 13% never change their password. Almost 40% of the entire crowd judged the effectiveness of social media sites in addressing and preventing cyberbullying or harassment as' somewhat effective', with 24% rating 'effective', 8.8% rating 'very effective', and 26.4% rating not effective.

FINDINGS

The study examines the various facets of privacy, highlighting how it is changing in the digital era. It looks at privacy from a number of angles, including legal, ethical, and technical, emphasizing the intricate relationship that exists between people's rights and society goals. The paper explores the difficulties brought about by information technology breakthroughs, including algorithmic profiling, data collection, and monitoring, which have a significant impact on privacy norms and behaviors. The study also examines how privacy violations affect people, businesses, and democratic institutions, highlighting the necessity of strong protections and legal frameworks.

The function of technologies to improve privacy and security by design concepts in reducing privacy threats and giving people the power to reclaim control over their private information is also covered. The research also highlights the significance of multidisciplinary teams and stakeholder participation to tackle complex privacy concerns in a quickly expanding digital ecosystem. It also indicates current trends and potential paths in privacy policy and research.

CONCLUSION

Serious privacy concerns have been brought up by the widespread usage of social media platforms, which has prompted an analysis of how these platforms affect users' digital identities and personal information. This study has shed light on the complex issues surrounding these concerns, which range from data breaches and unlawful access to information about users to the monetization of personal data for personalized advertisements. The analysis of prior research and empirical findings has also contributed to this understanding. Moreover, the intricate interactions among user conduct, platform methods, and regulatory structures highlight the necessity of adopting a holistic strategy to tackle privacy concerns in the digital era. While new technologies like encryption and privacy-preserving features provide potential answers, cultivating a culture of digital proficiency and encouraging user empowerment in managing privacy settings are ultimately responsible.Stakeholders may work together to create a more open, accountable, and moral social media ecology that protects user privacy while promoting innovation and connectedness by acknowledging the intrinsic worth of privacy as a basic human right.

FUTURE SCOPE

Scope of the article on privacy and security aspects of social media could delve into new technologies such as blockchain and decentralized networks as possible solutions. Additionally, exploring the intersections of AI and privacy and the impact of regulations such as GDPR and CCPA on social media platforms can provide valuable insights. In addition, it would be important to analyze the changing attitudes of users towards privacy and the adoption of privacy-enhancing tools and platforms.

REFERENCES

- Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information sciences, 421, 43-69.
- Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., ... & Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. International journal of environmental research and public health, 19(16), 9960.
- Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. Computers in Human Behavior, 120, 106763.
- Lina, L. F., & Setiyanto, A. (2021). Privacy concerns in personalized advertising effectiveness on social media. SRIWIJAYA INTERNATIONAL JOURNAL OF DYNAMIC ECONOMICS AND BUSINESS, 5(2), 147-156.
- Househ, M., Grainger, R., Petersen, C., Bamidis, P., & Merolli, M. (2018). Balancing between privacy and patient needs for health information in the age of participatory health and social media: a scoping review. *Yearbook of medical informatics*, *27*(01), 029-036.
- Quan-Haase, A., & Elueze, I. (2018, July). Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *Proceedings of the 9th international conference on social media and society* (pp. 150-159).
- Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *new media & society*, *20*(1), 141-161.
- Nuzulita, N., & Subriadi, A. P. (2020). The role of risk-benefit and privacy analysis to understand different uses of social media by Generations X, Y, and Z in Indonesia. *The Electronic Journal of Information Systems in Developing Countries*, *86*(3), e12122.
- Costello, C. R., McNiel, D. E., & Binder, R. L. (2016). Adolescents and social media: pPrivacy, brain development, and the law. *Journal of the American Academy of Psychiatry and the Law*, *44*(3), 313-321.
- Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal*, *18*(1), 48-58.
- Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *IEEE Security & Privacy*, *5*(3), 40-49.
- Steinberg, S. B. (2016). Sharenting: Children's privacy in the age of social media. *Emory Lj*, *66*, 839.
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, 106260.
- Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management (OJAKM)*, *7*(1), 1-13.
- Osatuyi, B. (2015). Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems*, *55*(4), 11-19.
- Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center*, *21*(1055), 2-86.