Social Media Manipulation and the Impact on Digital Security

A Research Paper Submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, VA

In partial fulfillment of the Requirements of the Degree

Bachelor of Science in Computer Science

Connor Wilson

Spring 2024

On my honor as a University of Virginia Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR:

William F. Stafford Jr., Department of Engineering and Society

Introduction

Love it or hate it, social media is here to stay. Since the early 2000's, social media has taken society by storm and completely changed the way that we interact with the world around us. With unprecedented collaboration that spans continents and cultures has come increasing concern that constant use of social networking sites and services are directly related to psychiatric disorders such as depression and addictive behavior (Pantic, 2014). Such concerns are commonly rooted in the belief that social media is slowly eroding the human element – that is the fellowship or connection we experience when in the presence of others. More and more people meet online instead of in person or text rather than talk on the phone. This pattern was only exacerbated by the COVID19 pandemic and corresponding forced isolation.

Amidst the entrenched presence of social media in our lives, another realm has emerged, one fraught with its own set of challenges and threats. As society became increasingly digitized the cyber domain rose in prominence, rapidly accompanied by the pressing matter of digital security. This entails safeguarding oneself or one's organization from malicious actors, colloquially known as "hackers," who seek to exploit vulnerabilities in hardware, software, or data without authorization. Since 2001, the estimated financial impact of cyber attacks on the U.S. information and communications technology (ICT) sector alone has been $188 million USD. Making that statistic even more sobering is that it is assuming only 10% inoperability in the sector as a result of those attacks. With an assumed inoperability of 40%, the statistic goes up to $564 million USD. On a global scale, the impact for the same time range easily clears a staggering $250 billion USD for the ICT industry alone (Dieye et al., 2020). Concerningly, cyber attacks were nowhere near their apogee a decade ago despite the increasing push for awareness (Bendovschi, 2015). Since then, it is estimated that poor digital security or the complete lack of

any digital security has cost the global economy $945 billion USD as of 2020 (Sharif & Mohammed, 2022). This is not to mention the incalculable cost rendered by the damage to affected businesses' reputations.

However, it is not just businesses that are affected by cyber attacks; cyber attacks can also devastate individuals. A single data breach can expose confidential user information including but not limited to credit card or bank account information, social security numbers, addresses, and names. This information can then be used by the perpetrator to steal a user's identity or can be sold to the highest bidder on the black market. Attacks can also target specific individuals to delete, steal, or ransom data that could have serious consequences for someone's life. Even on a small scale, ransomware encrypting every file on someone's personal computer can disrupt daily life, one's ability to do one's job, and potentially even compromise the digital security of the employer depending on if that user keeps work files on their personal device.

As social media becomes more ingrained into modern society's routines, it adds another level of complexity to the cyber threat landscape. As a technology that promotes communication and provides a platform with which to share information, social media is unique in its ability to disseminate messages rapidly and influence public discourse. However, this ubiquitous presence also presents an attractive target for malicious actors seeking to exploit vulnerabilities for nefarious purposes. The interconnected nature of social media platforms facilitates the spread of misinformation, amplifies the impact of cyber attacks, and complicates efforts to maintain digital security. Consequently, understanding the intricate dynamics of social media interactions is paramount for safeguarding individuals and organizations from potential threats.

In order to uncover the underlying mechanisms driving social media manipulation and the related implications for digital security, one can look to the conversation around such topics

for insight. A useful tool for evaluating how such conversations on and around social media are affecting the actions of users is conversation analysis (CA). CA is a framework included in the theory of Technological Mediation as described by Peter-Paul Verbeek in the 2015 Manhattan Papers (Verbeek, 2015). CA provides a framework through which to analyze how the conversation and sentiment surrounding a technology have an impact on the way that users interact with that technology as well as potential downstream effects of said interaction. In the context of this analysis, the technology in question is social media and the downstream effects would be the consequences of the way users interact with social media as they pertain to digital security.

In light of these considerations, this analysis will delve into the intricate ways in which social media influences users and potentially compromises their digital security. It will first explore several cases that provide a foundation to the claim that social media can exert influence on large groups of people in such a way as to have a significant impact on the collective behavior of the group. Subsequently, CA will be applied to those cases in order to examine motive, intent, method, and effect(s). Finally, the discussion will synthesize these findings, exploring their broader implications for both current and future scenarios and shedding light on the complex interplay between social media dynamics and digital security. For the purposes of this analysis, the scope will be limited to specific examples of social media manipulation and compromises of digital security in order to draw connections between the two broader topics, rather than a general discussion of the topics themselves.

The Intersection of Digital Security with Social Media

While not as popular on the evening news as phishing, ransomware, and other high profile attack types, there are many forms of cyber attacks that can use social media as a vector to exploit some service or device (Kunwar & Sharma, 2016). Sometimes, such threats are hiding in plain sight for anyone who is willing to take the time to look for them. One example comes from a study in which over 90% of users signing up to join a fictitious social networking service agreed to clauses buried in the Terms of Service (ToS) and Privacy Policy that gave the NSA permission to access all of the user's digital data. If that was not enough, each user also signed away the user's firstborn child as payment for using the service (Obar & Oeldorf-Hirsch, 2020). In other instances, users pose the biggest threat to themselves.

As for the aforementioned phishing and ransomware attacks, the list of affected companies and financial losses is quite extensive. Perhaps the most successful known phishing campaign to date is that of Evaldas Rimasauskas, a Lithuanian who tricked Google and Facebook into paying him an estimated $100 million USD over the course of two years. Rimasauskas was able to impersonate high level executives from Quanta Computer Inc., a Taiwan-based supplier of computer hardware for Facebook and Google, using emails where he sent Google and Facebook invoices, contracts, and other important documents that ultimately routed money to accounts owned by Rimasauskas (Pienta, et al., 2020). As for ransomware, a particularly relevant example is the Colonial Pipeline attack in 2021. The attackers were able to gain access through an unused account before gaining control of and shutting down the pipeline. In this case, that pipeline happened to be critical infrastructure for a vast portion of the East coast of the United States. Gas shortages quickly ensued while the pipeline was inactive, resulting in skyrocketing gas prices, shipping delays, and ultimately resulting in Colonial Pipeline paying the

attackers the 75 bitcoin (~$4.4 million USD at the time) ransom for reentry to their system. Ultimately, the Colonial Pipeline attack had significant impacts and implications not only for critical infrastructure security in the United States but also served to alarm other nations and consider how their infrastructure may be vulnerable (Beerman, et al., 2023).

While attacks like these are not strictly related to social media, they are made feasible by attack surfaces being developed by a world that is increasingly connected via a complex combination of fiber optic cables and vast computer networks. This is of course not to say that the costs outweigh the benefits of our world's digitalization, but it is a problem that if not addressed will continue to take larger tolls on society. Now that the stage is set, a new player enters stage left: social media.

This increased complexity in the cyber threat landscape ushered forth by social media is particularly easy to see in the gathering of open source intelligence (OSINT). In the context of this analysis, OSINT involves “the collection, analysis, and use of data from open sources for intelligence purposes” (Koops et al., 2013). OSINT can take a variety of forms but is most notable in a security context for its ability to enable various cyber attacks. As social media has grown, it has not only become a vector for digital attacks but has also become a medium through which to profile targets for future cyber attacks or other malicious actions. The bottom line is, whether it is knowingly or unknowingly, users are increasing their risk level every time they post something or interact with something on social media (Martinez-de-Morentin, et al., 2021).

Less tangible than OSINTs effect on digital security is social media’s power to influence. It is well documented that social media has the power to influence individuals or even more importantly groups to think or act in a desired way (Qin et al., 2011, Vollenbroek et al., 2014). The influencing force in such situations can range from large organizations like political

campaigns to individual influencers who have the capability to rapidly reach a massive base of followers (Fujiwara et al., 2023, Vollenbroek et al., 2014). One distinctly interesting example of social media being used to manipulate users is found in X (at the time named Twitter) being used as a medium through which users were influenced by U.S. presidential campaigns. Fujiwara, et al. (2023) found that there was a significant negative effect on the Republican vote share in both the 2016 and 2020 presidential elections as a result of political campaigning on Twitter. Most notable from this research is the claim that one in every twelve active Twitter users who voted for Presidential Candidate Hillary Clinton in 2016 may not have voted the same way if not for Twitter (Fujiwara et al., 2023). This study takes a highly mathematical approach to supporting that claim, but ultimately that approach is centered around the correlation between a drastic increase in Twitter users in the decade leading up to that election and a high volume of conversation about the election. In this case, the majority of that conversation was in support of the 2016 Clinton campaign and therefore was able to change vote share (Fujiwara et al., 2023). This is a perfect example of CA in that the discussion surrounding the election as allowed by a social networking service (Twitter) changed the way that users interacted with the world around them.

In that vein, part of what makes analyzing and predicting such relationships in social media so difficult is the existing ardor associated with discerning misinformation on social networking services (Muhammed & Mathew, 2022). While many social media companies have content policies, user verification measures, and content verification measures in place it can still be extremely hard to catch every piece of misinformation. Further muddying the waters is the fact that many people may not be intentionally spreading misinformation but rather repeating something they heard as true or presenting their own opinion as fact. A hot topic in the modern

discourse on social media, the qualifications for what qualify as protected free speech and what social media platforms sould or should not censor are highly debated and likely will continue to be for years to come.

In addition to the difficult nature of determining misinformation, the environment is further complicated by the power individuals can hold. In an environment where one user can have hundreds of millions of followers who consistently watch said user's content, having even a fraction of those followers' trust provides immense power to influence not only the thoughts but actions of a large group of people. A fantastic example of this phenomenon can be seen with TikTok, the social media platform owned by ByteDance that took the world by storm during the COVID19 pandemic. The rise of social media influencers has for the first time made it possible for anyone with a phone and something to say to reach other users en masse and change organizational images and reputations in the eyes of the public (Vollenbroek et al., 2014).

How does all of this relate back to digital security? It means users can be influenced to make choices, make purchases, or take actions that may compromise their digital security. In this vein, TikTok provides a fascinating case study. Despite numerous published concerns about ByteDance's collection and use of nonpublic user data in addition to its rumored connections to the People's Republic of China (Trump, 2020, Congressional Research Services, 2023, Vergun, 2023), many users still choose to use TikTok (Pew Research Center, 2022). In the following sections this analysis will strive to answer the question of why users continue to willingly engage with something that has been consistently received criticism as a cyber risk and even within the last 12 months was labeled a "potential threat vector" to the U.S. at large by the principal cyber advisor to the U.S. Secretary of Defense (Vergun, 2023).

Conversation Analysis and Influence

CA itself is very much related to sociology/group psychology (Heritage & Stivers, 2012). In one study on the effects of social influence on acceptance of online social networks, a mathematical relationship was found between the subjective norm and critical mass as they relate to social media, perceived usefulness, and usage intention (Qin et al., 2011). Subjective norm refers to a person's perception of the social expectations to adopt a particular behavior and is influenced by a person's normative beliefs combined with the person's motivation to comply (Peters & Templin, 2010). Critical mass is slightly easier to define as it is purely mathematical and refers to the minimum amount required to start something (Marwell et al., 1988). In this case, the intersection of both statistics provides an empirical foundation to illustrate the relationship between influence and actions taken as a result of that influence. This research is particularly apt because not only is it focused on social pressure as it pertains to social media but it is also the mathematical support for frameworks like CA that are less empirical by nature.

With that knowledge, the context of politics and specifically elections is an especially interesting realm to look at through the lens of CA as an integral component of modern elections is the campaign. At their core, political campaigns are simply a forum or platform for candidates to speak with the goal of influencing people to vote for them. The earlier example of Twitter's role in the 2016 and 2020 U.S. presidential elections becomes particularly interesting in the context of a 2017 meta-analysis of 76 studies, the results of which suggest that despite a drastic increase in political advertising on social media in the last decade (Tabini, et. al, 2017) social media has a minimal contribution to citizens' political knowledge (Amsalem & Zoizner, 2023). The combination of a high volume of conversation surrounding things like political campaigns with minimal educational benefits being seen despite such volume seems indicative of the intent

of those campaigning. Considering the empirical evidence supporting social media's ability to influence groups and social media's rising popularity it seems unlikely that users are not seeing social media traffic for political campaigns. More likely is the possibility that this phenomenon is reflective of the intent of those publishing the media.

This situation with social media is not unique to campaigns and elections. The TikTok discussion has a slightly more tangible connection to security but conversion in and around TikTok can also provide valuable insights into the intent of popular users and groups on the platform as well as that of ByteDance itself. One noteworthy area of discussion regarding TikTok is its utilization as a marketing platform. TikTok has been identified as the best form of mass media to create brand awareness from both a social and empirical perspective (Mutiara & Putri, 2023). TikTok's strategy for user retention is heavily based on personalizing the user experience by collecting as much user data as possible to use as input to the TikTok algorithm. That data may include but is not limited to clicks, time spent on various content creators or videos, and user habits on the platform to deliver tailored content, making for a quite addicting platform (Borges, 2023, Mutiara & Putri, 2023). Additionally, TikTok provides advertisers with the option to target demographics that include but are not limited to specific age groups, gender, and geographic location (Somosi et al., 2023). The ability for targeted advertising and the user experience created by the content suggestion algorithm provide a plausible explanation for TikTok's high user uptake and user retention, especially combined with the empirical findings suggesting that once a critical mass is achieved there is social pressure to participate in the platform (Qin et al., 2011). From a CA perspective, this is especially interesting because of the competing social pressure to join TikTok juxtaposed with the rampant security concerns associated with the platform. Once again, it raises the question of which conversation is

prevailing and why. This raises further questions: are seeing multiple perspectives? If not, are they becoming polarized in their beliefs? Does that benefit the content creator or ByteDance? What is the intent?

While these two cases may seem disconnected from one another except for the fact that they both relate to social media, they actually intersect to underscore a stark reality: social media's power to influence is both pervasive and potentially perilous. These cases raise critical questions about the prevailing narratives and users' perceptions of those narratives. Empirical findings combined with the application of CA tell us that despite its outward appearance as informative content, much of the content we are consuming on these platforms is not actually serving to teach us anything but rather to persuade us about something. In the case of elections the intent of that persuasion seems rather obvious, but this pattern is not limited only to elections. With TikTok, users are casting off the values of privacy and security for access to content of all sorts. In both cases, CA makes the underlying theme clear: social media's ability to shape opinions and behaviors poses significant risks as users navigate a landscape where influence often eclipses informed decision-making.

Discussion

The ability of social media platforms like TikTok or X (Twitter) to draw in and retain users is ultimately what enables them to influence users in cases like that of the 2016 and 2020 U.S. presidential elections. In the case of TikTok, aside from the influence it is able to exert to retain users on the platform, individuals who are content creators have the ability to reach massive user groups in seconds or minutes. While this is mostly in reference to influencers with many thousands if not millions of followers, TikTok's algorithm specifically allows content from

creators who may not have very many followers to get views and reach the critical mass of followers necessary to be influential at an astounding pace, many of those users coming from a younger generation (Somosi et al., 2023).

Were a content creator to post something that appealed specifically to a radical group of individuals incentivising them to take some action, what kind of traction could that gain and how many of those individuals would actually stop to think about the motivation behind that post? On a similar note of concern is the content sharing tendencies of the younger age group that accounts for most of social media users. One study done on Spanish youth ages 11-17 suggests that individuals in that age group are extremely confident in their own ability to detect disinformation, yet despite that are still highly likely to share that disinformation if it allows them to be part of a trend (Zozaya-Durazo et al., 2023). The natural follow up question is one of values – whether or not users value social status/convenience over truth when engaging with social media. If the former is true, it would be exceedingly easy to manipulate said users into using a malicious application that provides a seemingly innocent service. If the percentage of users who stop to read ToS or the privacy policy are any indication (Obar & Oeldorf-Hirsch, 2020), it is not a big step to assume that many users may not take the time to consider the risk if they see everyone they follow on social media using the application. Alternatively, even if they are concerned, they may succumb to social pressure once the user base hits the critical mass necessary to exert said pressure (Qin et al., 2011).

Another possibility is that users are simply not educated enough on the potential cyber threats they may face and as a result take uninformed actions online. This possibility is especially worrying in the context of social media because an uninformed audience is one that is much easier to influence. This thought is supported by the 2020 Pew Research Center findings

suggesting those who are mainly using social media for news are significantly more likely to be uneducated, more likely to see a lot of content relating to unproven stories such as conspiracy theories, and are less concerned about the impact of news that has been fabricated (Mitchell et al., 2020). Remarkable about the education dilemma is that while much of the existing research relating to social media is on younger age groups (Zozaya-Durazo et al., 2023, Pew Research Center, 2022, Mitchell et al., 2020), there is also research indicating that older users are less likely to secure their devices than younger users yet nonetheless are more proactive in their personal security posture (Branley-Bell et al., 2022). This likely should not come as a surprise considering that many older users did not grow up with the internet while those in Generation Z (1997-2012) and younger do not know what a world without the internet looks like. When put side by side, these findings suggest that the adolescent and elderly populations are the most affected by lack of education with a group in between that was likely introduced to the internet in their early childhood and therefore possesses the technical capacity and maturity to have a better understanding of the cyber threat landscape.

Finally, and potentially most concerning, is the possibility that users understand and simply do not care. Studies like the previously mentioned one that measured time spent reading ToS and privacy policy on a fictitious social networking service (Obar & Oeldorf-Hirsch, 2020) provide some insight into the phenomenon. Contracts and the importance of a signature are things that, at least in the U.S., are extremely common in education, business, and everyday life and consequently are understood as important by most individuals. However, when confronted with documents pertaining to their usage of a service and where their data is going they are often not reading it unless forced to (Obar & Oeldorf-Hirsch, 2020, Steinfeld, 2016). One possibility is that of the value of convenience being valued over security. ToS and privacy policies are often

long, wordy documents that take five minutes or more to read all the way through and fully understand. For many users, the priority seems to be accessing the service or application they are trying to use rather than reading these documents. The same logic can easily be applied to services, devices, or applications as well. One topic getting a lot of attention right now is the internet of things (IoT) and whether users value the convenience of IoT devices like Amazon Alexa or a smart refrigerator over the security concerns associated with them (Jaspers & Pearson, 2022, Jeon & Lee, 2022). The IoT, while groundbreaking and incredibly convenient, is ultimately just creating a larger attack surface for those who use it. It is not even infeasible that users continuing to use TikTok is a matter of convenience in the minds of many. At the end of the day, it is of course up to the user to determine and to strike the balance of convenience and security with any digital product or service one engages with.

The intricate interplay between social media dynamics and digital security underscores the urgent need for comprehensive understanding and proactive measures. As we navigate the evolving landscape of social media influence and its implications for cybersecurity, critical questions emerge. How do users perceive and respond to the pervasive influence of social media platforms? What factors shape their decisions and behaviors in the face of cybersecurity risks? These questions highlight the complex intersection of individual choice, societal norms, and technological developments. By delving into the nuances of social media manipulation and its impact on digital security, one can gain valuable insights into the challenges and opportunities ahead. As we strive to address these issues, it becomes increasingly clear that fostering digital literacy, promoting informed decision-making, and implementing robust security measures are essential steps in safeguarding individuals and organizations in an increasingly interconnected world.

Conclusion

Social media has changed the way that the world interacts over the past couple of decades. From Facebook to TikTok, social media platforms and social networking services have simultaneously created a more connected world and a more vulnerable world, affecting not only the human element of fellowship and physical interaction but the security of our nations and communities. The discussion above presents the argument that key in evaluating this relationship is considering the influence social media can now exert on individuals and groups and the downstream effects of such influence on security. More precisely, social media presents a more acute threat to a user's digital security when said user is uneducated on how to steward their own digital security and when users consider their own convenience more pressing than their digital security. The objective of this discussion is to both increase awareness of how social media can be used to influence users and to prompt further discussion on ways that these issues can be addressed. The future implications of a national or global society that is unaware of how the media they consume alters or governs their actions are grave not only for the security implications of such a scenario but also for the geopolitical landscape at large. Ultimately, the desire is that the above discourse will inspire consequential future discussions and research.

References

Amedie, J. (2015). The Impact of Social Media on Society. *Pop Culture Intersections*. https://scholarcommons.scu.edu/engl_176/2

Amsalem, E., & Zoizner, A. (2023). Do people learn about politics on social media? A meta-analysis of 76 studies. *Journal of Communication*, *73*(1), 3–13. https://doi.org/10.1093/joc/jqac034

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Borges, N. P. (2023). *User gratifications in social media usage: The case of TikTok* [masterThesis]. https://repositorio.ucp.pt/handle/10400.14/41410

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, *23*(2), 183–208. https://doi.org/10.1111/rmir.12151

Enríquez, J. R., Larreguy, H., Marshall, J., & Simpser, A. (2024). Mass Political Information on Social Media: Facebook Ads, Electorate Saturation, and Electoral Accountability in Mexico. *Journal of the European Economic Association*, jvae011. https://doi.org/10.1093/jeea/jvae011

Fujiwara, T., Müller, K., & Schwarz, C. (2023). The Effect of Social Media on Elections: Evidence from the United States. *Journal of the European Economic Association*, jvad058. https://doi.org/10.1093/jeea/jvad058

Heritage, J., & Stivers, T. (2012). Conversation analysis and sociology. *The handbook of conversation analysis*, 657-673.

Jaspers, E. D. T., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255–265. https://doi.org/10.1016/j.jbusres.2021.12.043

Jeon, H., & Lee, C. (2022). Internet of Things Technology: Balancing privacy concerns with convenience. *Telematics and Informatics*, *70*, 101816. https://doi.org/10.1016/j.tele.2022.101816

Koops, B.-J., Hoepman, J.-H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, *29*(6), 676–688. https://doi.org/10.1016/j.clsr.2013.09.005

Kunwar, R. S., & Sharma, P. (2016). Social media: A new vector for cyber attack. *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, 1–5. https://doi.org/10.1109/ICACCA.2016.7578896

Martinez-de-Morentin, Juan-ignacio, Lareki, Arkatiz, & Altuna, Jon. (2021, January 25). *Risks Associated With Posting Content on the Social Media*. https://ieeexplore.ieee.org/abstract/document/9335021?casa_token=HuIGyVEbyJcAAAAA:e2Ek057o-MPiE2-JOEBhmu-gUgP1TeEEzk_gBvgxrhL8lhNwALwwrMhpLY3cmGC_Lpqtwt6_Eg

Marwell, G., Oliver, P. E., & Prahl, R. (1988). Social Networks and Collective Action: A Theory of the Critical Mass. III. *American Journal of Sociology*, *94*(3), 502–534. https://doi.org/10.1086/229028

Mitchell, A., Jurkowitz, M., & Shearer, E. (2020, July 30). *Americans who mainly get their news on social media are less engaged, less knowledgeable*. Pew Research Center's Journalism Project. https://www.pewresearch.org/journalism/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeable/

Muchnik, L., Aral, S., & Taylor, S. J. (2013). Social Influence Bias: A Randomized Experiment. *Science*, *341*(6146), 647–651. https://doi.org/10.1126/science.1240466

Muhammed T, S., & Mathew, S. K. (2022). The disaster of misinformation: A review of research in social media. *International Journal of Data Science and Analytics*, *13*(4), 271–285. https://doi.org/10.1007/s41060-022-00311-6

Mutiara, P., & Putri, K. Y. S. (2023). Uses and Gratification Theory in TikTok as Social Media Marketing Platform: Seen from Market Player View. *Journal of Digital Marketing and Communication*, *3*(1), Article 1. https://doi.org/10.53623/jdmc.v3i1.164

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Peters, R. M., & Templin, T. N. (2010). Theory of Planned Behavior, Self-Care Motivation, and Blood Pressure Self-Care. *Research and Theory for Nursing Practice*, *24*(3), 172. https://doi.org/10.1891/1541-6577.24.3.172

Qin, L., Kim, Y., Hsu, J., & Tan, X. (2011). The Effects of Social Influence on User Acceptance of Online Social Networks. *International Journal of Human–Computer Interaction*, *27*(9), 885–899. https://doi.org/10.1080/10447318.2011.555311

Sharif, M. & Mohammed, M. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Pantic, I. (2014). Online Social Networking and Mental Health. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 652–657. https://doi.org/10.1089/cyber.2014.0070

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of information technology*, *35*(3), 214-231.

Somosi, Z., Hajdú, N., & Molnár, L. (2023). Targeting in Online Marketing: A Retrospective Analysis with a Focus on Practices of Facebook, Google, LinkedIn and TikTok. *European Journal of Business and Management Research*, *8*(1), Article 1. https://doi.org/10.24018/ejbmr.2023.8.1.1724

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior*, *55*, 992-1000.

Tambini, D., Labo, S., Goodman, E., & Moore, M. (2017). The new political campaigning. *Media policy brief*, *19*.

Trump, D. (2020). *Executive Order on Addressing the Threat Posed by TikTok – The White House*. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

Verbeek, P. P. (2015). Toward a theory of technological mediation. *Technoscience and postphenomenology: The Manhattan papers*, *189*.

Vergun, D. (2023). *Leaders Say TikTok Is Potential Cybersecurity Risk to U.S.* U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3354874/leaders-say-tiktok-is-potential-cybersecurity-risk-to-us/

Zozaya-Durazo, L. D., Sádaba-Chalezquer, C., & Feijoo‐Fernández, B. (2023). “Fake or not, I’m sharing it”: Teen perception about disinformation in social networks. *Young Consumers*. https://doi.org/10.1108/YC-06-2022-1552