Protecting privacy on social media platforms: a case study of Croatian users

Anamarija Horvat, Renata Mekovec
University of Zagreb Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
ahorvat21@student.foi.unizg.hr, renata.mekovec@foi.unizg.hr

Abstract. *This study identifies three areas of research that are investigated in relation to privacy protection when using social media platform: (1) technical area, (2) area related to the user and (3) area related to privacy models. A survey was done to find out how much privacy awareness Croatian users of social media platform have. The results show that a lot of users of social media platforms share their first and last names, photos and videos, and their birth date. The research uncovered also significant security gaps like a limited awareness of basic security measures and a significant lack of awareness about the rights users have in the context of privacy protection.*

Keywords. privacy concerns, social media platform, digital threats

1 Introduction

Billions of people utilize major social media platforms such as Facebook, Instagram, TikTok, Snapchat, YouTube, Twitter, and LinkedIn. A total of 5.52 billion people were using the internet at the start of October 2024, where number of internet users have increased by 151 million (+2.8 percent) over the past 12 months. According to Kepios's latest analysis, the number of social media platform users is equating to 63.8 % of all the people on Earth (Kemp, 2024).

Social media platform's phenomenal expansion has provided their owners with unprecedented access to and control over users' lives. Social media platforms collect information like personal data, demographic information, interests, behaviors, and activities elsewhere on the internet (Federal Trade Commission, 2024). Some of this information is willingly supplied via posts and profile information. Information also may be released unknowingly through tracking cookies, which track a user's online activities such as webpage visits, social media platform sharing, and purchase history. All information is then collected and organized into user categories, which data brokers sell for marketing purposes.

On other hand it should be stressed that social media platforms have drastically changed perceptions about privacy. While technology allows self-expression and virtual interactions, it also introduces hazards such as profiling, targeted advertising, and mass monitoring. It is true that cyberbullying, and data breaches have a significant impact on confidence in the digital economy. Trust in online services, and social media platforms declines when people suffer from data breaches or are the targets of cyberbullying and online bullying. People may be less inclined to consume digital goods, reveal personal information, or participate in online activities as a result of this diminished confidence (ENISA, 2024).

The combination of AI, analytics, behavioral science, social media platform, Internet of Things (IoT) and other technologies makes an incredible opportunity for bad actors to create and spread highly effective, mass-customized disinformation, also known as malinformation (Plummer et al., 2023). Americans have little faith that social media platform executives will responsibly handle user privacy. Approximately 77% of Americans don't trust social media platform executives to speak up with their mistakes and accept accountability for misuse of their platforms. Furthermore, they have lost faith in the government's capacity to control them: 71% of people don't think the government will hold these tech CEOs responsible for their mistakes. Although the majority of Americans (85%) believe that parents bear a major portion of the duty for safeguarding their children's online privacy, they also believe that tech corporations (59%) and the government (46%) bear this obligation (Pew Research Center, 2023). Only half Europeans believe their digital rights are well secured, over a third feel the EU isn't doing enough, and 45% are unsatisfied with the protection of children in the digital environment. The lowest percentage, at just 40%, believes they have full control over their own data and digital legacy. Older respondents are more likely to believe the EU does not protect their rights adequately in the online environment. Those aged 40-54 are the most likely (38%) to think this, followed by those aged 55 and up (36%). Younger respondents (15-24) are less likely to support this opinion (32%). For example, 73% of those aged 15-24 believe that getting more freedom of expression and information online e.g., via online

platforms, social networks, search engines is well protected in their country (European Union, 2023).

While some experts stated that people are extremely worried about their online privacy, others suggested that, while being sceptical of social media platform practices, users were willing to reveal personal information in exchange for tiny advantages (Khan et al., 2023). The "privacy paradox" phenomenon proposes that users of social media platforms who are highly concerned about their privacy do not always apply their concerns to their usage practices. In other words, despite their high level of privacy concerns, social media platform users continue to utilize the platform in their daily lives (Hew et al., 2019).

The challenge of protecting privacy when utilizing social media platforms is one that both researchers and the IT sector struggle with. As stated by TechTarget (2024) common social media platform privacy issues include: (1) data mining for identity theft, (2) vulnerabilities in privacy settings (loopholes), (3) location settings, (4) harassment and cyberbullying, (5) fake information, and (6) malware and viruses.

The research described in this paper aims to better understand the current perspective on privacy protection on social media platforms, from an academic and social media platform user's standpoint.

Therefore, this research is to address following research questions:

1. what is the latest research on protecting privacy on social media platforms?
2. how can privacy be protected on social media platforms?
3. what is the level of privacy awareness among Croatian social media platform users?

The primary contribution of this work is to identify most recent research on privacy protection when using social media platforms in order to use this knowledge to improve user privacy awareness. This will be performed by reviewing the most recent academic results, investigating practical privacy protection methods, and analysing the level of privacy awareness among Croatian social media platform users.

2 Recent studies regarding privacy on social media platforms

Researchers concentrate on various privacy areas, privacy issues, and privacy protection strategies used by social media platform users. Thus, they focus on fatigue due to social media platform (Dhir et al., 2019), usage intention (X. Fan et al., 2021), (Neves et al., 2024), (Garima & Sheokand, 2024), users' lurking behavior (Liu et al., 2024), most important preferences of users regarding social media platform apps (Alshehri & Alamri, 2022), (Bracamonte et al., 2024), (Tang & Ning, 2023), the effectiveness of social media platform advertising (Jung & Heo, 2024), privacy differences across various regions (Farooq et al., 2024), (Meso et al., 2021), (Nuzulita & Subriadi, 2020).

The aim of this study was to find the most important studies on privacy challenges when using social media platform and identify the main research area addressed by the aforementioned studies.

2.1 Review methodology

The research articles included in this study were published between 2019 and 2024 and retrieved from Scopus and Web of Science. These databases were chosen because they contain the most recent full-text peer-reviewed publications, have advanced search capabilities, and cover the most published research papers. The following keywords were used in a keywords-based search method: "social media" AND "privacy concern". The quantity of citations of the publications was taken into account while selecting important papers, and some of the most widely referenced articles in our study (Table 1) were selected as seed papers. In the second step, a graph-based search strategy was utilized to locate more relevant papers, with papers found during our initial search serving as seeds. To make the graph more focused on subject, we begin adding articles that we find important. Citation analysis tools Inciteful (https://inciteful.xyz/) was used to create citation network graphs, and to explore and add most important recent related papers to the database. In total 204 items in all were gathered in this manner.

Table 1. Most widely referenced articles in our study – seed papers

Title	Cited
The age of mobile social commerce: An Artificial Neural Network analysis on its …(Hew et al., 2019)	199
Antecedents and consequences of social media fatigue (Dhir et al., 2019)	190
Privacy concerns and benefits of engagement with social media-enabled apps: ….(Jozani et al., 2020)	170
Effect of penitence on social media trust and privacy concerns: The case of … (Ayaburi & Treku, 2020)	119
The role of trust and privacy concerns in using social media for e-retail services: …(Alzaidi & Agag, 2022)	82
Does role conflict influence discontinuous usage intentions? Privacy concerns.. (X. J. Fan et al., 2021)	49
Social media users' online subjective well-being and fatigue: A network … (Kaur et al., 2021)	47

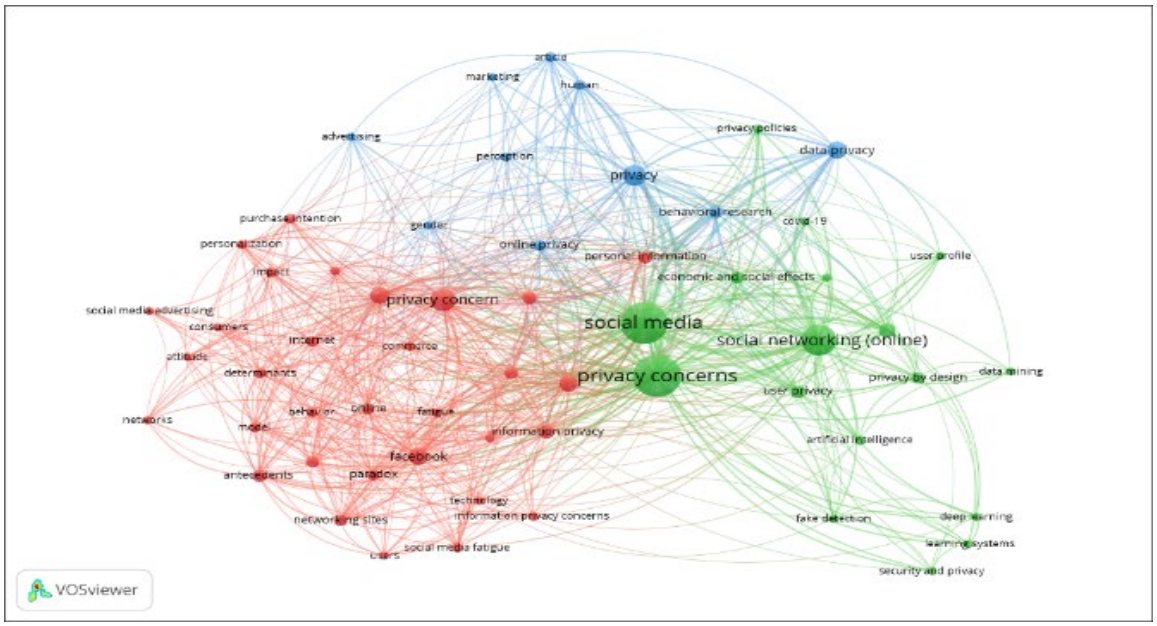

Figure 1. Keyword co-occurrence network map

Fig. 1 displays a keyword co-occurrence map of selected articles (204 articles/items identified in second step) derived by bibliometric analysis in VOSViewer. In the network visualization, items are represented by their label and by a circle. The size of the label and the circle of an item is determined by the weight of the item. The higher the weight of an item, the larger the label and the circle of the item is. The colour of an item is determined by the cluster to which the item belongs. Lines between items represent links.

On the visualization of related keywords, it can be seen the grouping of keywords around three clusters. In this manner it can be answered on research question: what is the latest research relevant to privacy on protecting privacy on social media platform? Considering the structure of keywords in each cluster, it can be defined that research focus is on: (1) technical area, (2) area related to the user and (3) area related to privacy models. The first cluster, the **technical area**, includes technology that is increasingly being used in all aspects of life, thus affecting social media platforms as well. It is thus evident that research related to privacy in the field includes issues related to artificial intelligence, data mining, learning systems, as well as fake detection and privacy by design. The second cluster, the **area related to the user**, is oriented towards users of social media platforms, so research in this area is focused on perception, behavioral research, gender and personal information. The third cluster, **the area related to privacy models**, includes research related to antecedents and determinants of privacy concerns, paradox, model and impact.

3 Methods for privacy protection on social media platform

In the context of increasing digital threats, privacy protection on social media platforms has become a crucial topic. This chapter presents key methods of protection that social media platform users can apply, along with an analysis of recommendations from relevant sources and experts.

3.1 Using complex and unique passwords

The complexity of passwords and avoiding predictable patterns are crucial for security. According to MacKay (MacKay, 2024), passwords that combine uppercase and lowercase letters, numbers and symbols and exceed 12 characters in length significantly reduce the risk of compromise. Passwords that include personal information such as names or birth dates should be avoided, as such data is easily accessible through social media platform, making the account more vulnerable to attacks.

3.2. Implementation of two – factor authentication (2FA)

Two – factor authentication adds an extra layer of protection. According to Counting Up (How to Maintain Privacy on Social Media | Countingup, 2022), the introduction of one – time login codes, in addition to regular passwords, reduces the risk of unauthorized access. This measure provides additional security because an attacker cannot gain access to the account without possessing the codes specific to the user's device, which significantly reduces the risk of hacking.

3.3. Adjusting privacy settings

Controlling privacy settings and regularly adjusting the visibility of personal data are essential protective measures. According to recommendations given by Data Privacy Manager (How to Protect Your Privacy on Social Media? – Data Privacy Manager), users should limit the visibility of their profiles to options such as „friends“ and „only me“ to reduce the risk of information misuse. This adjustment allows users greater control over who can see their information, thereby reducing the possibility of privacy compromise.

3.4. Access management: forced logout and login monitoring

Forced logout from devices and regular checking of active logins are important security step. MacKay (MacKay, 2024) emphasizes that control over active sessions allows users to detect unknown devices and quickly remove unauthorized users from the account. This measure ensures that users have insight into active devices, which improves access control and reduces the risk of account compromise.

3.5. Deleting old and inactive accounts

Old, inactive accounts often remain vulnerable to attacks because users rarely update their security settings. Bizga (2023) recommends deleting these accounts and requesting from platform administrators to remove all associated personal data from these accounts. By doing so, users reduce the „attack surface” since inactive accounts are often not protected by modern security measures.

3.6. Preventing excessive sharing of personal data

The European Commission (Komisija, n.d.) recommends refraining from sharing excessive personal data, including sensitive information such as exact locations and personal photos. This practice can prevent potential misuse, especially when it comes to sensitive data about locations and daily activities. Additionally, the Commission advises adopting a selective approach to accepting friend requests and engaging with unknown individuals to further reduce the risk of data misuse.

Establishing strong privacy protection on social media platforms require users to consistently adhere to security guidelines and utilize available tools. Regularly updating privacy settings, deleting old accounts, using complex passwords and implementing two – factor authentication significantly reduces the risk of personal data compromisation. These measures, combined with education about threats, such as phishing attacks and cyberbullying, are essential for enhancing security on social media platforms. In the broader context, digital security awareness and responsible digital behavior become crucial components in combating increasingly sophisticated cyber threats, thereby contributing to overall safety on online platforms.

4 Analysis of research results

As part of the preparation for the undergraduate thesis „Privacy protection on social media platform“ a research study was conducted to examine the security practices, privacy awareness and attitudes of Croatian social media platform users regarding digital threats and personal data protection (Horvat, 2024). The primary objective of the study was to: (1) assess the respondents’ level of awareness about security threats, (2) identify patterns in social media platform usage and protective measures and (3) analyse the ways personal data is shared on these platforms.

Questionnaire consist form 35 questions where answers were proposed. First group of questions were demography characteristic like gender, age and working status, usage of social media platform (awareness, daily usage in hours, device from which is social media platform accessed and what social media platforms is used by respondents). Second group of questions were connected to information that respondents are sharing via social media platform (Which types of information do you share on social media platforms?), with whom are they sharing information (Who are your followers on social media platforms, or with whom do you share information?), who are they follow (Whose friend requests/follow requests via social networks do you accept?) what information are they revealing (Whether and how often you publish your location on statuses, posts, videos or photos you post on social media platforms?). Third group of questions was connected to security measures that respondents use:

1. Do you use the same password for more social media platforms?
2. Are your passwords longer than 12 characters?
3. Do you use a combination of upper and lower case letters and a combination of numbers and/or characters and symbols (eg ?, !, ,, ., *, +, -) in your password for social media platforms?
4. Do you, and how often, connect different social media platforms through the same account (e.g. connecting Facebook and Instagram accounts)?
5. How old were you when opened your Facebook profile?

Fourth group of questions encompass following items:

1. Have you ever experienced a situation where your privacy was compromised when using social media platform, such as hacking profile or identity theft?
2. Are you familiar with the term GDPR (General Data Protection Regulation)?
3. Are you familiar with the term "Digital Fingerprint"?
4. Have you ever received a certain type of spam messages via social media platform (e.g., advertisements for products and services, messages that encourage certain religious or political opinion)?
5. Have you ever been a victim of "phishing", or online identity theft? (A person persuades a victim to reveal personal information via a link to a fake website and then uses the victim's information and poses as that person)
6. Have you ever been a victim of stalking via social media platform?
7. Have you ever been a victim of bullying via social media platform (e.g., insults, mockery, threats)?

Fifth group of questions encompass items connected to awareness of protecting during online activities:

1. Do you know what two-factor authentication is and do you use it when logging in to your social media platform?
2. Are you deleting profiles on social media platforms that you no longer use?
3. Do you know that only uninstalling certain social media platform applications will not delete your profile and posts that did you post?
4. Did you know that there are tools today that allow people to, by simply entering any photo you've posted on social media platform, find out when the photo was taken, where it was taken, and find the people in it?
5. Do you know how to set the visibility of personal data on social media platform posts and profiles to "only me" or "friends" and remove the option to find information about you using your email or social media platform link?
6. Do you know how to find devices that are logged into your profile and log out of those that don't belong to you?
7. Do you know that you have the right to ask the data controller a copy of the data collected about you, to whom all these data are sent, what is the purpose of this sending and request deletion of data after a certain period of time, if there is no reason for them to be detained?
8. Do you know what AZOP (Personal Data Protection Agency) is and what you can report to it?
9. Are you using any kind of antivirus protection?
10. Do you think that more should be said and people should be taught about privacy protection on social media platforms?

The research sample was made using snowball sampling method, and have consisted of Croatian users, providing insights into security practices within a specific cultural and legal framework. However, the conclusions were limited to the regional context, serving as a basis for comparison with global trends in digital security.

The sample included 140 respondents from the Republic of Croatia, of which 65% were women and 35% men. The respondents were predominantly young, with half of the total sample being aged between 18 and 25 years, 17.9% aged between 36 and 45 years, while the remaining portion of the sample was older than 46 years. The largest segment of respondents consisted of college students (47.1%), followed by employed individuals (37.9%), with high schoolers, unemployed and retirees being represented in smaller numbers (12.9%, 1.4% and 0.7% respectively). This structure provided insight into the behavioral patterns and attitudes of the population most active on social media platform in Croatia, with a particular focus on young users and their security and privacy practices.

The research revealed that 98.6% of respondents use social media platforms, while only 1.4% are aware of it but do not use it. The time spent on social media platform is also significant: 40.7% of respondents use social media platform between two and four hours daily, 24.3% from one to two hours, 23.6% spend between four and six hours on social media platform and the remaining 10% spend more than six hours on them daily, thus increasing their exposure to potential threats. Access to social media platform is predominantly through mobile devices (92.9%), while the use of laptops and desktop computers is minimal (3.6% and 2,1% respectively), highlighting the need for specific security measures tailored to mobile platforms.

The most frequently used social media platforms among respondents are WhatsApp (96.4%), YouTube (82.9%), Instagram (78.6%) and Facebook (68.6%), while platforms like X (Twitter) (12.9%) and Skype (9.3%) are less popular. This segment of the research indicated that the surveyed users are primarily focused on platforms that enable communication and multimedia content sharing.

The results show that 86.4% of respondents publicly share their first and last names on social media platform, 74.3% share photos and videos, while 58.6% share their birth date. Additionally, 36.4% of respondents share their phone number, increasing the

possibility of identity theft or contact misuse by malicious users. None of the respondents indicated sharing financial information or personal identification numbers, which suggests a basic level of awareness regarding the protection of sensitive information. However, it also highlights vulnerability due to sharing data such as phone numbers and birth dates.

The questions aimed at understanding privacy threats covered respondents' perceptions of risks such as hacking, cyberbullying and phishing attacks. The results show a high level of concern among respondents: 70% express worry about potential privacy breaches, while 50% are concerned about hacking and the misuse of personal data. Despite these concerns, the research uncovered significant security gaps; 43.6% of respondents use the same passwords across multiple platforms and 60.7% use passwords shorter than twelve characters, making them vulnerable to brute – force attacks and other forms of cyber threats. Only 68.6% of respondents use antivirus protection, indicating a limited awareness of basic security and privacy measures.

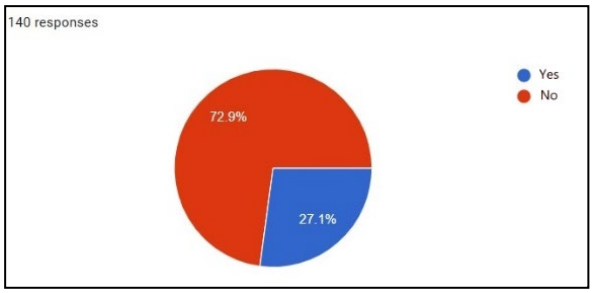

Figure 2. 5. Have you ever been a victim of "phishing", or online identity theft? (Horvat, 2024)

Questions related to the perception of threats, such as cyberbullying, profile hacking and phishing, indicate a limited understanding of these dangers. Fig. 2 shows results of question related to profile hacking or identity theft. Respondents answered that as many as 27.1% of them experienced profile hacking or identity theft, which proves that they should be educated about ways to protect against repeated attacks. Also, approximately 45% of respondents reported that they have personally experienced, or know someone who has experienced, cyberbullying, while 52% understand the danger of phishing attacks but are unsure how to recognize them. These results highlight the need for specific educational interventions aimed at recognizing and protecting against digital threats.

Questions regarding users' legal rights revealed a significant lack of awareness about the rights users have in the context of privacy protection. Specifically, 58.6% of respondents did not know they could request a copy of their data stored by social media platforms, while 56.4% were unaware of the role of the Croatian Personal Data Protection Agency (AZOP). This low level of awareness highlighted the need for additional informational campaigns to help users better understand their rights and the legal framework for privacy protection in the digital space.

Fig. 3 shows the results related to the final question of the research, specifically about their opinion on the importance of education and discussions about privacy protection on social media platform. As many as 96.4% of respondents believe that there should be more discussions and education about privacy protection on social media platform. This indicates that the respondents are aware of the need for greater public awareness of online privacy protection methods and that the research itself has prompted them to reassess their own privacy.

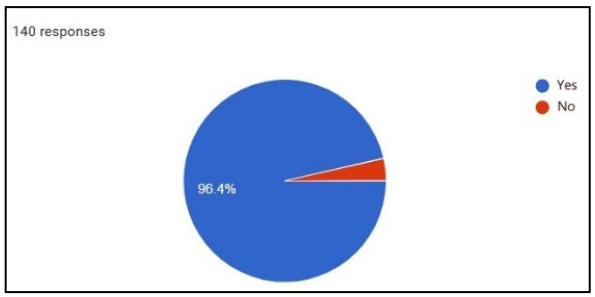

Figure 3. 10. Do you think that more should be said and people should be taught about privacy protection on social media platforms? (Horvat, 2024)

5 Conclusion

The overall results of performed research indicate a high level of social media platform usage among Croatian users, but reveal an insufficient level of applied security and privacy measures and an insufficient level of awareness of threats such as hacking, cyberbullying and phishing attacks. Despite concerns about security and privacy, a significant portion of respondents do not undertake basic security measures, such as using unique and complex passwords and multi – factor authentication. Additionally, the research reveals a low level of awareness regarding rights to access and control over personal data.

Given the identified vulnerabilities, it is recommended to introduce specific educational initiatives focused on basic security practices and user rights. Campaigns should include recognizing threats such as phishing attacks and cyberbullying, using complex and unique passwords, the importance of antivirus tools and the implementation of multi – factor authentication. Additionally, it is necessary to educate users about legal rights concerning data protection and privacy control, in collaboration with initiatives such

as AZOP, enabling users to better understand and apply security measures.

The results of this research, though limited to a national sample, provide insights into security attitudes that align with European trends. Younger generations exhibit high engagement on social media platform but limited awareness of advanced security practices. The findings of the research are an important contribution to understanding national attitudes towards digital security and privacy, highlighting the need for an interdisciplinary approach and international cooperation in promoting a culture of digital security on a global scale.

References

Alshehri, A., & Alamri, S. (2022). Exploring Social Media Privacy Preferences in Saudi Arabia. *International Journal Of Computer Science And Network Security*, *22*(1), 725–730. https://doi.org/10.22937/IJCSNS.2022.22.1.95

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal Of Retailing And Consumer Services*, *68*. https://doi.org/10.1016/j.jretconser.2022.103042

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal Of Information Management*, *50*, 171–181. https://doi.org/10.1016/j.ijinfomgt.2019.05.014

Bizga, A. (2023). *Why you should delete old accounts you no longer use*. https://www.bitdefender.com/en-us/blog/hotforsecurity/why-you-should-delete-old-accounts-you-no-longer-use

Bracamonte, V., Orito, Y., Fukuta, Y., Murata, K., & Isohara, T. (2024). Perception of Privacy Tools for Social Media: A Qualitative Analysis Among Japanese. In D. V. S.De.C. & S. P. (Eds.), *Proceedings of the International Conference on Security and Cryptography* (pp. 151–162). Science and Technology Publications, Lda. https://doi.org/10.5220/0012762000003767

Dhir, A., Kaur, P., Chen, S., & Pallesen, S. (2019). Antecedents and consequences of social media fatigue. *International Journal of Information Management*, *48*, 193–202. ENISA. (2024). *Foresight Cybersecurity Threats for 2030* (Issue March). https://doi.org/10.2824/349493

European Union, Special Eurobarometer 532, The Digital Decade, https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=88016

Europska Komisija, *Zaštitite svoju privatnost na društvenim mrežama*. https://ec.europa.eu/croatia/secure_privacy_on_social_networks_hr

Fan, X. J., Jiang, X. Y., Deng, N. Q., Dong, X. B., & Lin, Y. X. (2021). Does role conflict influence discontinuous usage intentions? Privacy concerns, social media fatigue and self-esteem. *Information Technology & People*, *34*(3), 1152–1174. https://doi.org/10.1108/ITP-08-2019-0416

Fan, X., Jiang, X., Deng, N., Dong, X., & Lin, Y. (2021). Does role conflict influence discontinuous usage intentions? Privacy concerns, social media fatigue and self-esteem. *Information Technology & People*, *34*(3), 1152–1174. https://doi.org/https://doi.org/10.1108/ITP-08-2019-0416

Farooq, A., Salminen, J., Martin, J. D., Aldous, K., Jung, S. G., & Jansen, B. J. (2024). Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries. *IEEE ACCESS*, *12*, 147087–147105. https://doi.org/10.1109/ACCESS.2024.3463869 WE - Science Citation Index Expanded (SCI-EXPANDED)

Federal Trade Commission. (2024). *A Look Behind the Scenes Examining the Data Practices of Social Media and Video Streaming Services* (Vol. 4, Issue 2). https://doi.org/10.36950/apd-2016-011

Garima, & Sheokand, K. (2024). Demystifying the Effect of Social Media Advertising on Purchase Intention of Millennials: Role of eWOM and Privacy Concerns. *JOURNAL OF CREATIVE COMMUNICATIONS*. https://doi.org/10.1177/09732586241246403

Hew, J.-J., Leong, L.-Y., Tan, G. W.-H., Ooi, K.-B., & Lee, V.-H. (2019). The age of mobile social commerce: An Artificial Neural Network analysis on its resistances. *Technological Forecasting & Social Change*, *144*, 311–324. https://doi.org/https://doi.org/10.1016/j.techfore.2017.10.007

Horvat, A. (2024). *Zaštita privatnosti na društvenim mrežama | Repozitorij Fakulteta organizacije i informatike*. https://repozitorij.foi.unizg.hr/islandora/object/foi:8166

How to Maintain Privacy on Social Media | Countingup. (2022). https://countingup.com/resources/how-to-maintain-privacy-on-social-media/

How to Protect Your Privacy on Social Media? – Data Privacy Manager. Retrieved December 19, 2024, from https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/

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*. https://doi.org/10.1016/j.chb.2020.106260 WE - Social Science Citation Index (SSCI)

Jung, A. R., & Heo, J. (2024). How Did You Get My Information? The Influence of Personal Information Gathering Methods on Social Media Advertising Effectiveness. *International journal of human-computer interaction*, *40*(20), 6579–6590. https://doi.org/10.1080/10447318.2023.2258019

Kaur, P., Islam, N., Tandon, A., & Dhir, A. (2021). Social media users' online subjective well-being and fatigue: A network heterogeneity perspective. *Technological Forecasting And Social Change*, *172*. https://doi.org/10.1016/j.techfore.2021.121039

Kemp, S. (2024). *The Global State of Digital in 2024 — DataReportal – Global Digital Insights*. https://datareportal.com/reports/digital-2024-october-global-statshot

Khan, M. I., Loh, J., Hossain, A., & Talukder, M. J. H. (2023). Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users. *Computers In Human Behavior*, *142*. https://doi.org/10.1016/j.chb.2022.107638

Liu, X. Y., Feng, R., Chen, X. B., & Yuan, Y. (2024). "Left on read" examining social media users' lurking behavior: an integration of anxiety and social media fatigue. *Frontiers In Psychology*, *15*. https://doi.org/10.3389/fpsyg.2024.1406895

MacKay, J. (2024). *How to Protect Your Personal Information on Social Media*. https://www.aura.com/learn/how-to-protect-your-personal-information-on-social-media

Meso, P., Negash, S., & Musa, P. (2021). Interactions between Culture, Regulatory Structure, and Information Privacy across Countries. *Journal of Global Information Management*, *29*(6). https://doi.org/10.4018/JGIM.20211101.oa49

Neves, J., Turel, O., & Oliveira, T. (2024). Explaining Social Media Use Reduction As an Adaptive Coping Mechanism: The Roles of Privacy Literacy, Social Media Addiction and Exhaustion. *Information Systems Management*. https://doi.org/10.1080/10580530.2024.2332187

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. *Electronic Journal of Information Systems in Developing Countries*, *86*(3). https://doi.org/10.1002/isd2.12122

Pew Research Center. (2023). *How Americans View Data Privacy*.

Plummer, D., Karamouzis, F., Alvarez, G., Hill, J., Sallam, R., McMullen, L., Sicular, S., Ramsey, M., Andrews, W., Bittman, T., Gupta, R., Scheibenreif, D., Raskino, M., Henein, N., Moyer, K., Furlonger, D., Johnson, B., Markkanen, A., Jones, L., … O'Donohue, R. (2023). *Gartner's Top Strategic Predictions for 2024 and Beyond — Living With the Year Everything Changed*. *November 2023*. https://www.gartner.com/doc/reprints?__hstc=254338199.dfb32abfb3189962387122c6e2bbd286.1704311186728.1704311186728.1704311186728.1&__hssc=254338199.8.1704311186728&__hsfp=1654019965&id=1-2FZ2U5YZ&ct=231218&st=sb&submissionGuid=4c21bbc0-5ce2-42d7-a424-8517

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems*, *165*. https://doi.org/10.1016/j.dss.2022.113881

TechTarget. (2024). *6 Common Social Media Privacy Issues | TechTarget*. https://www.techtarget.com/whatis/feature/6-common-social-media-privacy-issues