



RESEARCH ARTICLE

Navigating Privacy and Cultural Identity: Social Media Use and Privacy and Security Concerns among Saudi Youth

Shoeb Saleh^{1*}, Tarik N. Mohamed²

¹The National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia.

¹Department of Educational Technology, Faculty of Education, Sohag University.

²Department of Global Studies, Business School, KFUPM, Dhahran, Saudi Arabia.

²IRC for secure, intelligent systems, KFUPM, Dhahran, Saudi Arabia.

ARTICLE INFO

ABSTRACT

Received: Sep 17, 2024

Accepted: Nov 22, 2024

Keywords

Social Media

Privacy

Security

Saudi Youth

Digital Literacy

Cultural Context

Gender Differences

Online Behaviors

In recent years, social media platforms have become deeply embedded in daily communication, offering new opportunities for virtual connection and community. However, these platforms also introduce significant privacy and security risks for users. This study explores the effects of social media usage on the privacy and security perceptions of Saudi university students, a demographic that is increasingly active on these platforms. A sample of 900 undergraduate students from various public universities across Saudi Arabia participated, providing valuable insights into privacy attitudes within this cultural context. The findings reveal a notable correlation between the frequency of social media use and concerns related to privacy and security, indicating that higher engagement often correlates with increased awareness of privacy vulnerabilities. Additionally, the study found significant gender differences in privacy perceptions, with male and female participants. Differences were also observed across academic disciplines, where students in certain fields demonstrated greater confidence and awareness in online privacy and security practices than others. These results highlight the influence of social media use on Saudi students' views about privacy and highlight the importance of cultural and educational factors in shaping these perceptions. The study contributes to a nuanced understanding of how social media impacts privacy awareness within specific cultural settings. Findings support the need for tailored digital literacy programs to improve privacy and security awareness among young adults, fostering safer online behaviors as social media usage continues to grow.

*Corresponding Author:

sgsaleh@kfu.edu.sa

INTRODUCTION

Social media has become an integral part of daily life, representing a broad spectrum of web and mobile platforms where users can interact within virtual networks. These platforms, including popular ones like Snapchat, X, Instagram, and TikTok, enable users to share, create, and exchange various types of digital content—such as messages, images, videos, and general information—thereby redefining social interactions on a global scale (Ahmed et al., 2019; Naslund et al., 2020). With this convenience comes a host of privacy concerns, as users often trade personal information for enhanced and personalized services. This pattern of behavior reflects a tension between users' awareness of privacy risks and their psychological tendencies to continue sharing personal details online, suggesting a direct relationship between individual privacy desires and online social behavior.

The demarcation between public and private spheres has become increasingly ambiguous, requiring social media users to manage their online identities strategically to mitigate risks to personal privacy.

As the lines between public and private spaces blur, social media users are increasingly faced with choices about how to balance these spaces and implement security measures to protect sensitive information (Kenton et al., 2022).

One of the key factors influencing how individuals manage their privacy online is the inherent variability in privacy values. Users attribute different levels of significance to privacy based on personal values, lifestyle, and personality traits, which, in turn, influence their online activities and the extent of personal disclosures. For instance, Ryan and Xenos (2011) examined social network behaviors through the lens of the Big Five personality traits and identified four major categories of Facebook activities: active social contributions, passive engagement, news and information sharing, and real-time interactions. Their findings suggest that social media behaviors are closely linked to individual personality traits, which determine the extent to which users engage with content and participate in online communities. This insight has been corroborated by several studies investigating privacy from a multidimensional perspective, which include not only the well-known aspects of information and communication privacy but also physical, decisional, and psychological privacy concerns (Fuchs, 2022). Koops (2017) advanced this understanding of privacy by categorizing it into eight types: physical, geographic, communicative, proprietary, intellectual, choice, associative, and behavioral privacy. These dimensions highlight that privacy is a complex, multifaceted construct, extending well beyond simple data protection to encompass various aspects of individual autonomy, identity, and security.

Technological advancements, especially in the realm of biometric systems, have added layers of complexity to privacy concerns. Retinal scanning, facial recognition, fingerprint systems, and other biometric tools offer new ways to secure user data and facilitate seamless online experiences, but they also present unprecedented risks by infiltrating spaces once deemed personal and secure. For example, facial recognition technology is now able to analyze facial features and expressions, capturing more than just identity but also revealing emotional responses, which raises concerns about psychological privacy. Similarly, systems analyzing body sensations, eye movements, and other biometric data bring questions of privacy and consent to the forefront (Gu, 2020). These advancements enable hackers and other malicious actors to exploit these technologies, leveraging biometric data to infiltrate individuals' private lives. For instance, hackers may use location-tracking features on social media platforms to deduce users' home addresses or frequently visited locations, thus compromising physical and geographic privacy. These challenges highlight the need for social media users to be vigilant and adopt proactive privacy measures, particularly for those who frequently engage with online platforms.

The current study aims to explore these critical privacy concerns in the context of Saudi Arabian youth, focusing on their engagement with popular social media platforms and the associated impacts on privacy and security.

Saudi Arabia represents a unique setting for such an investigation due to its distinct cultural values and the rapid social transformations it has undergone in recent years (Mohamed & Bendania, 2024; Abdelrheem & Bendania, 2022). In Saudi society, traditional values rooted in Islam emphasize family cohesion and close-knit social relationships. As a result, the family unit is regarded as one of the most essential social institutions, influencing many aspects of individual behavior and identity formation. Social media usage within this cultural context presents a particular set of challenges. For example, while young Saudis may use platforms like Instagram or Snapchat to connect with friends and family, they often avoid disclosing information that could be perceived as infringing upon family privacy or going against social norms (Askool, 2012). This inclination toward family-centered interactions contrasts with the openness and visibility encouraged by many social media platforms, where sharing personal achievements, social connections, and lifestyle details are common. Long (2005) emphasizes that while Saudis have traditionally preferred to display social connections with family members rather than strangers, modernization and increased interaction with global cultures have begun to shift these behavioral patterns, particularly among the youth.

The rapid digital transformation in Saudi Arabia, driven by increased access to the internet and higher levels of education, has led to an exponential rise in social media use among young people. This increased usage has contributed to new patterns of behavior that reflect a complex blend of

traditional values and modern digital practices. As young Saudis become more active on social networks, they experience a shift in how they perceive privacy and approach the balance between online presence and cultural expectations. These shifts in behavior, influenced by both educational attainment and greater exposure to global trends, have significant implications for understanding privacy within Saudi society. Many young Saudis now use platforms like Twitter, Instagram, and TikTok not only to connect with friends and family but also to engage with wider online communities and access information beyond their immediate social circles. However, as social media becomes more ingrained in their lives, these users encounter heightened privacy risks that arise from the need to navigate both personal and cultural expectations in a public, digital space.

In this context, privacy concerns extend beyond individual preferences to reflect broader cultural and social norms. Saudi society places a high value on respect for privacy, especially within the family setting. However, the rise of digital technology has introduced new pressures for Saudi youth to conform to both local customs and the globalized behaviors associated with social media usage. This dual pressure creates a tension that requires users to carefully manage their online image while safeguarding personal information. Privacy is not a monolithic concept but rather a variable one shaped by multiple factors, including culture, social expectations, and individual personalities. For Saudi youth, maintaining a balance between self-expression and adherence to cultural norms is crucial, especially as they navigate platforms that often encourage openness and public visibility.

Moreover, gender differences play a notable role in privacy management on social media in Saudi Arabia. In Saudi culture, gender norms significantly influence social interactions, and this extends to digital platforms as well. Female users, for instance, may face additional scrutiny regarding their online presence, leading them to adopt more conservative privacy settings or engage in selective sharing to conform to societal expectations. Male users, while also mindful of privacy, may have more leeway in terms of online visibility. These gender-based differences highlight the diverse ways that Saudi youth approach social media privacy, often adopting unique strategies to ensure they adhere to both personal preferences and cultural expectations.

The current study aims to investigate these complex privacy dynamics, focusing on the experiences and perceptions of Saudi youth as they engage with social media. It seeks to understand how young Saudis navigate privacy concerns in a context where cultural norms are rapidly evolving due to modernization and increased global exposure. By examining privacy and security concerns through the lenses of gender, frequency of social media use, and academic discipline, this research aims to shed light on the factors that shape privacy management among Saudi youth. For instance, students from fields related to technology and information science may have a greater awareness of online privacy risks and adopt more robust privacy measures compared to those in non-technical fields. Similarly, frequent users of social media may develop specific strategies for privacy protection based on their experiences and awareness of platform vulnerabilities.

The findings from this study will contribute to a more understanding of how social media usage affects privacy concerns within the Saudi cultural context. Given the unique blend of traditional values and modern influences shaping Saudi society, this research offers valuable insights into the privacy practices of Saudi youth as they navigate the digital landscape. In addition, by focusing on variations across gender and academic disciplines, the study provides a comprehensive perspective on the factors that influence privacy management strategies among Saudi social media users. This research aims to inform future policy recommendations and digital literacy programs designed to promote safer online behaviors and privacy awareness in Saudi Arabia. Ultimately, understanding the privacy concerns of Saudi youth in the context of social media usage has implications not only for Saudi society but also for global discussions on privacy in digital spaces where cultural diversity and individual preferences interact.

METHODS AND PROCEDURES

This study employs a correlation methodology to explore the relationship between social media use and privacy and security concerns among Saudi university students. In line with ethical standards, careful consideration was given to participant consent, data collection, and cultural adaptation of instruments.

Ethical considerations

This study followed the American Psychological Association (APA) Ethical Principles of Psychologists and Code of Conduct to ensure a responsible and ethical approach to research involving human participants. In adherence to these guidelines, participants were informed of the study's objectives, data collection procedures, and confidentiality protocols via an introductory statement provided in the online survey. To confirm voluntary participation, students were asked to indicate their consent by selecting "Yes" to participate or "No" to decline. Only those who provided affirmative consent were included in the study. Confidentiality was emphasized, with clear assurances that participants' responses would be anonymized and used solely for research purposes. These measures ensured ethical compliance and respected participant autonomy.

Participants

The study sample included 900 college students recruited from various public universities in Saudi Arabia, providing a diverse representation of the Saudi student population. Of these participants, 499 were male (57%), and 401 were female (43%), reflecting a nearly balanced gender distribution. Students from all academic levels—first-year, sophomore, junior, and senior—were included, adding to the representativeness of the sample in terms of educational stage. Prior to participation, each student read and signed an informed consent form that detailed the study's purpose and their rights as participants, confirming their free will to take part in the research.

Study instruments

The study employed two primary instruments: the Online Social Network Form and the Online Privacy and Security Questionnaire. These tools were selected and adapted to provide a comprehensive assessment of participants' social media habits, privacy concerns, and security practices.

Online social network form

The Online Social Network Form was developed by the researcher to capture participants' habits and behaviors on social media. This form includes 8 items focused on various aspects of social media usage, such as time spent on platforms, frequency of engagement, types of activities (e.g., posting, commenting, and sharing), and primary social media platforms used. The form was designed with the cultural context in mind to ensure relevance to Saudi students' social media experiences.

To establish reliability, the form was piloted with a sample of 280 participants who completed it twice over a 15-day interval. This test-retest method produced a correlation coefficient of 0.77, indicating satisfactory reliability. The form's concise structure and relevant content made it suitable for efficiently collecting data on social media behaviors within the study's target population.

Online privacy and security questionnaire

Privacy and security were assessed using a modified version of the Online Privacy and Security Questionnaire originally developed by Georgia Tech University in 1998. The original questionnaire was adapted to better fit the cultural and social context of Saudi Arabia, particularly to address privacy concerns specific to this demographic. Several items that were culturally irrelevant or inappropriate were removed, ensuring the questionnaire's relevance to Saudi students.

The modified questionnaire contains 27 items in a Yes/No format, divided into two subcategories: privacy (14 items) and security (13 items). To facilitate use among Arabic-speaking participants, the questionnaire was translated into Arabic through a back-translation process, ensuring linguistic accuracy and cultural appropriateness. The final Arabic version was distributed via Microsoft Forms, a widely accessible platform for Saudi university students.

Reliability for the questionnaire's dimensions was measured using the Guttman split-half reliability coefficient. The security dimension yielded a reliability score of 0.79, while the privacy dimension showed a reliability score of 0.77. The overall reliability of the modified questionnaire was 0.68, demonstrating acceptable internal consistency for the study's purposes.

Procedures

The study was conducted in four distinct phases, designed to ensure comprehensive data collection and validation of study instruments.

Phase I: Instrument validation

In the initial phase, the instruments were validated with a preliminary sample of 300 students. This phase was crucial for confirming the reliability and appropriateness of the Online Social Network Form and the adapted Online Privacy and Security Questionnaire. The feedback from this pilot group helped fine-tune the items and ensure that both tools were effectively capturing the intended constructs. Adjustments were made to enhance clarity, and additional instructions were provided to address any areas of confusion reported by the pilot participants.

Phase II: Distribution of the online social network form

In the second phase, the Online Social Network Form was distributed to the full study sample via a Microsoft Forms link. Participants from various public universities across Saudi Arabia received an invitation to participate in this stage, with instructions to generate a unique code for future follow-up communications. This code allowed the research team to match responses without collecting identifiable information, thus maintaining participant anonymity. The form included a detailed introduction that outlined the study's purpose and instructions for completion, and participants were encouraged to use personal email addresses rather than university-provided emails. This choice minimized any potential biases related to institutional affiliations and helped further protect participants' privacy.

Phase III: Distribution of the privacy and security questionnaire

After completing the Online Social Network Form, participants were sent a second link to access the Online Privacy and Security Questionnaire. A follow-up reminder was also sent to ensure that the maximum number of participants completed both instruments. The questionnaire was structured to allow easy navigation, with Yes/No questions enabling students to quickly indicate their privacy and security preferences without excessive cognitive load.

During this phase, the research team monitored response rates and addressed any technical issues encountered by participants. By distributing the two instruments separately, the study minimized potential fatigue effects and maximized the likelihood of thoughtful and accurate responses.

Phase IV: Data analysis and interpretation

In the final phase, data from both instruments were compiled and subjected to statistical analysis. Descriptive statistics were calculated to summarize demographic information and basic trends in social media use, privacy, and security concerns. Correlational analyses were conducted to examine relationships between social media usage patterns and privacy/security concerns. Additionally, t-tests and ANOVAs were performed to explore potential differences in privacy and security concerns by gender and academic discipline.

This systematic approach allowed for a nuanced examination of the data, revealing patterns and insights relevant to the study's research questions. The results provided a clear understanding of how Saudi university students perceive and manage privacy and security issues in the context of social media, offering valuable insights into gender- and discipline-based variations in these concerns.

RESULTS

As shown in table (1), the relationship between online social network, Online security, and Online privacy were examined by calculating correlation coefficient. It has been noted that there is a correlation between varied factors.

Table 1: Correlation coefficients between study variables

	Networks	Privacy	Security
Social media Platform	1.00		
Privacy	-0.719**	1.00	
security	-0.693**	0.735**	1.00

As shown in table (2) there were significant differences in the scores of online social networks, Online security, and online privacy between male and female participants. Specifically, female students got higher scores than male participants in online social network use, online privacy, and security. According to the difference comparison results and earlier analysis, it could be concluded that gender played a moderating role in the relationship between the use of online social networks and information privacy and security.

Table 2: Differences between males and females in study variables

	Male		Female		t	Sig
	Mean	SEM	Mean	SEM		
networks	5.38	0.98	6.16	1.01	3.546**	0.001
Privacy	4.29	0.89	4.86	0.93	3.061**	0.010
security	4.01	0.87	4.35	0.91	2.988**	0.010

As shown in table (3), the differences in privacy, and security were examined depending on the frequency of online social media use. The online social network use frequency was categorized into three distinct categories. Category I for those who spend 3 hours or more daily on online social media. Category II, those who spend 1 to 3 hours on online social media. Category III, those who spend less than 1 hour daily on online social media.

One-way ANOVA revealed a significant difference between distinct categories in privacy, and security with different patterns. Results showed that those individuals who spend less than an hour a day showed high concern about security and privacy.

Table 3: Differences in study variables depending on the social network use

	Category I		Category II		Category III		F	Sig
	Mean	SEM	Mean	SEM	Mean	SEM		
Privacy	5.110	0.8900	4.590	0.860	4.640	0.840	6.921**	0.001
Security	6.960	0.9900	5.960	0.930	5.260	0.890	4.869**	0.010

As shown in table (4), the differences in privacy and security were examined according to the participants' study discipline. Students' academic majors included three distinct categories: life science and medicine; humanities and social sciences; Science and Engineering. Data analysis revealed a significant difference between distinct categories in privacy with different patterns. Students from science and engineering majors showed greater concern about privacy than other majors.

Table 4: Differences in study variables depending on the major study type

	Life science and medicine (N= 198)		Humanities and social sciences (N=244)		Science and Engineering (N=258)		F	Sig
	Mean	SEM	Mean	SEM	Mean	SEM		
Privacy	5.910	0.9930	5.820	0.930	6.830	0.980	4.638**	0.001
Security	6.850	0.9800	6.640	0.970	6.740	0.960	0.892	0.452

GENERAL DISCUSSION

This study aimed to explore the impact of social media use on the privacy and security concerns of Saudi youth, focusing on the influence of social network usage on their awareness and behavior regarding online privacy and data security. As the digital landscape continues to evolve, social media platforms, such as Facebook, Instagram, TikTok, and Snapchat, have become integral aspects of daily life for millions of young individuals. These platforms provide numerous opportunities for personal

expression, social interaction, and entertainment. However, their widespread use has brought about increasing concerns related to personal privacy, data security, and online vulnerability, particularly among young users. This study sought to investigate how Saudi youth's engagement with social media platforms correlates with their perceptions of online privacy and information security, particularly considering various factors such as time spent on social media, gender, and academic discipline.

The research findings revealed several significant insights that contribute to the understanding of the relationship between social media usage and online privacy/security among Saudi youth. Specifically, the study tested hypotheses regarding the correlation between time spent on social media and levels of privacy/security, the impact of gender on privacy concerns, and differences based on academic disciplines. The results provide a deep understanding of how social media usage is connected to privacy and security perceptions in the context of Saudi youth.

Impact of time spent on social media on privacy and security

The first major hypothesis tested was the correlation between the amount of time spent on social media and the level of concern for privacy and security. The results indicated a negative correlation, meaning that as participants spent more time on social media platforms, their awareness of privacy risks and security concerns decreased. This finding suggests that individuals who use social media extensively tend to lower their guard when it comes to protecting their personal information. As young people become increasingly immersed in these platforms, they may begin to take privacy and security for granted, unintentionally exposing themselves to risks like identity theft, phishing attacks, or data breaches.

One explanation for this result is that social media platforms are designed to encourage users to share information freely. Features like status updates, photos, and location sharing promote a culture of openness, which can desensitize users to the risks of sharing personal information. For young people, especially, the appeal of connecting with others and building social networks may overshadow the awareness of potential privacy threats. Moreover, the constant exposure to social media can lead to a psychological desensitization to privacy concerns. With time, users may grow accustomed to disclosing personal details, such as their whereabouts, preferences, or even financial information, without fully understanding the long-term implications of these disclosures. This phenomenon highlights the need for increased digital literacy education, teaching young users not only how to navigate these platforms but also how to protect their digital identity and information.

Gender differences in social media usage and privacy concerns

Gender was another key variable examined in this study, and the findings revealed significant differences between male and female participants regarding both social media usage and privacy/security concerns. Female participants were found to use social media platforms more frequently than their male counterparts, a finding that aligns with existing research on gender differences in online behavior. Previous studies have suggested that women, in general, tend to engage more deeply with social networks, particularly in the context of building and maintaining social relationships. This may be particularly true in Saudi Arabia, where cultural norms often restrict face-to-face social interactions for women. The relative anonymity and the ability to control the extent of exposure online may encourage women to engage in more frequent social media use compared to men.

In addition to higher levels of social media usage, female participants in this study also expressed greater concern regarding online privacy and security. They reported being more cautious about sharing personal details online, particularly sensitive information such as financial data or personal identification information. This heightened concern could be attributed to several factors, including societal expectations of women in Saudi Arabia, who are traditionally expected to maintain higher levels of privacy and modesty. The cultural emphasis on protecting women's honor and dignity in public life may translate into a stronger inclination toward safeguarding personal information online. Furthermore, women are often more vulnerable to certain types of online threats, such as cyberstalking or harassment, which may increase their awareness and sensitivity to privacy issues.

The higher levels of concern for privacy expressed by female participants suggest that they are more attuned to the risks associated with oversharing on social media. This finding is in line with previous research that has shown that women are generally more cautious when it comes to online privacy than men. Women's awareness of the potential consequences of oversharing—such as being targeted for online scams or falling victim to cyberbullying—may drive their more vigilant approach to privacy on social media platforms.

Influence of academic discipline on privacy and security concerns

Another important variable explored in this study was the academic discipline of the participants. The findings revealed that students majoring in science and engineering exhibited greater concern for online privacy and security compared to their peers in other fields. Science and engineering students, by the nature of their studies, are often more exposed to technical knowledge about data security and digital vulnerabilities. They are more likely to be aware of the risks associated with online activity, such as hacking, phishing, and other forms of cybercrime. This technical awareness may make them more cautious and vigilant about protecting their personal data when using social media platforms.

In contrast, students in humanities and social sciences, as well as those studying life sciences and medicine, did not display the same level of concern regarding online privacy and security. This discrepancy could be explained by the varying levels of exposure to digital security topics across different disciplines. While students in the sciences may have received formal education or training in data protection and online security, students in other fields may not have had the same level of exposure to these critical issues. As a result, students in non-technical fields may not recognize the full extent of the risks associated with sharing personal information online. This finding suggests that targeted education programs that emphasize the importance of digital literacy and security could benefit students across a wide range of academic disciplines.

Additionally, the study found that students in the social sciences were more likely to engage in online social networking activities than their peers in other fields. This trend may be attributed to the nature of social science studies, which often emphasize human behavior, societal interactions, and communication. Social science students may be more inclined to use social media as a tool for networking, staying informed about current events, and engaging with others in their field. This increased engagement with social media could further expose social science students to privacy and security risks, making it all the more important for them to be aware of these issues.

CONCLUSION

In conclusion, the findings of this study highlights the critical importance of privacy and security awareness in the context of social media use. The negative correlation between social media usage and privacy/security concerns highlights the risks associated with excessive use of these platforms, especially among young people who may not fully recognize the potential consequences of oversharing personal information online. Gender differences in privacy concerns further emphasize the role of cultural and societal factors in shaping individuals' attitudes toward online privacy. Female participants, in particular, were found to be more cautious about online privacy, which may be influenced by cultural expectations regarding modesty and privacy in Saudi Arabia. The impact of academic discipline also played a significant role, with students in technical fields such as science and engineering demonstrating higher levels of privacy and security awareness compared to their peers in other disciplines.

Declarations

Funding statement: The authors acknowledge the Deanship of Scientific Research at King Faisal University, Saudi Arabia for financial support under annual research grant number GrantKFU242544.

Conflict of interest: The author declared no potential conflict of interest in connection with this article's research, authorship, and/or publication.

REFERENCES

- Abdelrheem, T. N. M., & Bendania, A. (2022). The Role of Actively Open-minded Thinking among College students and its impact on future time perspectives: The Role of AOT in FTP. *Acción Psicológica*, 19(1), 85-94.
- Ahmed, Y. A., Ahmad, M. N., Ahmad, N., & Zakaria, N. H. (2019). Social media for knowledge-sharing: A systematic literature review. *Telematics and Informatics*, 37, 72–112.
- Askool, S. (2012). An investigation of social media use in Saudi Arabia. In *WEBIST* (pp. 471-481).
- Chabrol, H., Laconi, S., Delfour, M., & Moreau, A. (2017). Contributions of psychopathological and interpersonal variables to problematic Facebook use in adolescents and young adults. *International Journal of High Risk Behaviors and Addiction*, 6(1), e32773. <https://doi.org/10.5812/ijhrba.32773>
- Fuchs, C. (2022). An alternative view of privacy on Facebook. *Information*, 2(1), 140–165. <https://www.mdpi.com/2078-2489/2/1/140/htm>
- Georgia Tech University. (1998). Online tools. https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/questions/privacy.html
- Gu, L. (2020). Integrated privacy: A new type of privacy in the era of big data. *Nanjing Social Sciences*, 4, 106–111+122.
- Kenton, W., Mansa, J., & Jackson, A. (2022). Understanding social networking. *Investopedia*. <https://www.investopedia.com/terms/s/socialnetworking.asp> (accessed June 29, 2022)
- Koops, B. J., & Galič, M. (2017). Conceptualizing space and place: Lessons from geography for the debate on privacy in public. In *Privacy in Public Space* (pp. 19–46).
- Liu, Y., Tse, W. K., Kwok, P. Y., & Chiu, Y. H. (2022). Impact of social media behavior on privacy information security based on analytic hierarchy process. *Information*, 13, 280. <https://doi.org/10.3390/info13060280>
- Long, D. E. (2005). *Culture and customs of Saudi Arabia*. Greenwood Press.
- Mohamed, T. N., & Bendania, A. (2024). Investigating the relationship of actively open-minded thinking in future time perspectives among Saudi undergraduate students. *Psychological Research*, 88(1), 222-237.
- Naslund, J. A., Bondre, A., Torous, J., & Aschbrenner, K. A. (2020). Social media and mental health: Benefits, risks, and opportunities for research and practice. *Journal of Technology in Behavioral Science*, 5(3), 245-257.
- Ryan, T., & Xenos, S. (2011). Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage. *Computers in Human Behavior*, 27, 1658–1664.
- Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In *Handbook of Information and Computer Ethics* (pp. 131–164). Rivier University.
- Vangeel, L., Trekels, J., Eggermont, S., & Vandenbosch, L. (2017). Adolescents' objectified view of their friends: The role of media use, an objectified self-concept, and online appearance conversations. In *Etmaal van de Communicatiewetenschap* (Date: 2017/01/26-2017/01/27, Location: Tilburg, the Netherlands).