

Examining the concepts of privacy and information security in Emirati society: A survey

Khalaf Tahat¹, Ahmed Mansoori², Dina Naser Tahat³,
Mohammad Habes⁴, Ihsan Maysari⁵, Najia Ketbi⁶, Noura Naqbi⁷

¹Media & Creative Industries Department, United Arab Emirates
University & journalism department at Yarmouk University, Jordan.
k.tahat@uaeu.ac.ae

²Media & Creative Industries Department, United Arab Emirates
University
a.mansoori@uaeu.ac.ae

³Applied Sociology, Al Ain University, UAE
dina.tahat@aaau.ac.ae

⁴Faculty of Mass Communication, Radio & TV Department, Yarmouk
University, Jordan.
mohammad.habes@yu.edu.jo

⁵Emirates News Agency, Abu Dhabi, UAE
wamiwam@hotmail.com

⁶Mohamad Bin Zayed University for Humanities
Najia.alketbi@mbzu.ac.ae

⁷Emirates College for Advanced Education
noura.alnaqbi6@hotmail.com

Abstract

Abstract: Privacy is the right of an individual to control their personal information and how it is used, whereas information security is the protection of data from unauthorized access, modification, or destruction. The aim of this paper is to highlight the issues of privacy and information security among the Emirati public who use social media. A questionnaire was administered to convenience sample of 218 participants. The results showed that Instagram was the most used, and Facebook was the least used among the sample members. In addition, the Emirati society enjoys a high level of understanding regarding the concepts of privacy and information security. The findings reveal that they surround themselves with 'thick boundaries' regarding sharing their personal information on their accounts on social media platforms. The results reveal that 68% of the study sample did not accept friend requests from people they that did not know, and

two-thirds did not use their real names in those accounts or share any information about their workplaces. The findings show no statistically significant difference between males and females in their perceptions of the concept of privacy on social media platforms.

Keywords: Privacy, Information security, Social media, UAE, Personal information.

Introduction

Scholars defined the concept of privacy in different way, Warren and Brandeis (1890) defined privacy as the “right to be let alone” (p. 75), Westin (1967) said that privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967, p. 7), and Altman (1975) defined privacy as “the selective control of access to the self” (p. 24). Today, social media platforms such as Facebook, Twitter, Instagram and Snapchat have become an important part of people's social lives, and many share personal news and opinions about what is occurring in their lives (Al Olaimat, Habes, Al Hadeed, and Jwaniat. 2022; Tahat, Elareshi, Tahat, Jwaniat, Habes, and Ziani, 2022).

The issues of privacy violations, awareness, and limits are critical concerns at the present time, especially with the increase in users of social networking sites. Information thieves and hackers are also increasingly in search of victims through spyware, deceptive links, or sending viruses to hack personal data, which enables hackers to have access to all personal information (Blumberg et al, 2016).

The risk of violating the privacy of users on social networking sites is increasing; these risks put researchers in the field of modern media before their responsibility to study the level and nature of users' awareness of social networking platforms regarding the concept of privacy and extent of their ability to manage their personal information and protect it from penetration and violation. This includes providing information on the risks associated with sharing personal information online, guidance on how to use privacy settings and security features effectively, and highlighting the importance of good digital hygiene (Gordon, Loeb, Lucyshyn, and Zhou, 2015; Wang, Habes, and Li, 2022).

Importance

This study derives its significance from the importance of social networking sites in our time, and their strong, active and influential influence in shaping, making and directing public opinion. In addition, it enables decisionmakers to view the reality of user's awareness on social networking sites regarding the concept of privacy in an objective scientific context, to take the appropriate procedural steps in dealing with the issue of privacy violations. In the scientific context, this study

uses a scientific theory that defines some concepts related to the research problem, especially because some of them have not been used before in Arab media studies, specifically the communication privacy management theory.

Statement of the problem

Despite the advantages of social networking sites in facilitating communication, acquaintance, trade, other activities, services and human relationships for individuals or institutions, other users were victims of these sites, as they fell into networks of fraud and criminal professionals due to a lack of awareness and a limited culture of use of these communication sites, especially in light of the high crimes of extortion, plagiarism, fraud, invasion of privacy and assault on the private lives of ordinary citizens.

At the UAE level and as part of the country's efforts in digital transformation, the number of active accounts on social media applications in the UAE until January 2023 was approximately 39 million (Global Media Insight report, 2023). The total number of users was approximately 10 million. YouTube, Facebook, TikTok, LinkedIn, Snapchat and Twitter are the most used applications in the UAE. The UAE is one of the countries witnessing an increase in cybercrime, and according to the annual Norton Cyber Security Insights report, 2.53 million people in the UAE were victims of cybercrime in 2015 (MENA Herald, 2016). Victims of cybercrime in the UAE lost five billion dirhams (Khan, Reza, Rakhman, Bangera, 2016).

Recently, the Dubai Police announced that about 26,000 people had used the force's cybercrime platform on its website to report cybercrime (Al-Amir, 24 August 2022). With the increase in violations and cybercrime, the federal government of the United Arab Emirates took the initiative to criminalize violators of users' privacy on social media platforms, and the Cybercrime Law (Federal Law No. 5 of 2012) considered it a crime punishable by imprisonment and large fines. This directed the research teams' attention toward investigating awareness of the Emirati public regarding the concept of privacy and information security when using social media platforms.

Objectives

The research team aims to achieve the following key goals:

- 1) Identifying the extent to which the Emirati public is aware of potential exposure in social networking sites.
- 2) Knowing the nature of the information that the user discloses on social networking sites, and the mechanisms for protecting user's personal information

3) Realizing the risks, benefits, and motives for involved in voluntary disclosure of personal information.

4) Knowing the statistically significant differences between the personal variables of the respondents and benefits of disclosing personal information.

Literature Review

In the most recent study about privacy in the UAE, Azzi and Dakhane (2022) studied used questionnaire tool on local residents, the results indicated that most of the sample (71 per cent) agreed that personal information should be private and confidential on social media. Home address, passport license, gender and mobile number as the most sensitive information for the sample (67 per cent).

Shahid and Abdulla (2021) aimed at enhancing awareness of privacy and security issues associated with social networks and providing guidance to users for the safe use of social websites. They used a questionnaire, and the results showed that most users had their real information on social networking sites and did not change the privacy settings of their accounts regularly; moreover, most of the users accepted friend requests and invitations from unknown people on social networking sites, and the respondents mentioned that they did not change the initial privacy settings on their accounts on those sites, and that they allowed public access to their personal data.

Katharine and Winter (2017) aimed to explore the ways in which users of virtual networks understood the concept of privacy regarding users' awareness of privacy policies and laws within legal dimension in terms of violations. By using focus groups, the results indicate that a common thread in the study was the idea that an individual's privacy is determined by the ability or lack of control over the presentation of their information. Overall, the study indicated that, during the focus group interviews, participants generally admitted that they had little or no understanding of privacy settings.

Faraj (2015) explored the attitudes of the Egyptian public towards a culture of privacy through social networking sites, and the advantages and risks of self-disclosure. The findings indicated that the higher the level of perceived risk among individuals by revealing their information on Facebook, the lower their rate of self-disclosure through the site.

Saeri, Ogilvie, La Macchia, Smith, & Louis (2014) examined the online privacy protection behaviour of Facebook users, considering the effect of perceived risk and trust on online privacy. The most prominent results were that the participants who were worried about protecting their privacy found that trust is related to attitudes and behaviours to protect privacy. Moreover, men were more confident in this than women, with 37 per cent checking their accounts daily. At the same time, 47 per cent

said they restrict access to their information because they are generally wary, and 38 per cent because they have heard of 'some' privacy breach stories.

Young and Quan-Haase (2013) examined the strategies that undergraduate students resorted to and their motivation to use specific strategies to protect their privacy. The results indicated that, in addition to using default privacy settings, students developed several strategies to meet their privacy needs including excluding contact information, using limited profile options, giving up photos, removing tags and limiting friend requests from strangers. Respondents disclosed a large amount of information that they usually share with others, including their birthday, place of birth, friends, photos and emails, as well as sensitive information, such as addresses, course schedules and phone numbers.

Boyd and Hargitay (2010) measured the attitudes and practices of a group of 18–19-year-olds in 2009 and again in 2010 regarding their Facebook privacy settings. The results showed that young people do not care about and do not deal with privacy; the data indicated that the general trend among young people regarding modifications to privacy settings has increased. The results of the study also indicated that women are more likely than men to change Facebook privacy settings compared to males, and women do so more often, indicating that women are more actively seeking to manage privacy.

Waters and Ackerman (2010) aimed to determine the expected motivations of voluntary disclosure by active Facebook users using a survey of American college students. The results showed that Facebook users use this predominantly to disclose information to distant friends than to close friends, which differs from the rest of the research that describes disclosure with close friends. The results also showed that there was a significant difference in the means between females ($M = 5.21$) who were more likely to agree that they were motivated to disclose on Facebook through information storage and entertainment than men ($M = 3.88$). Results showed that individuals who use Facebook to disclose private information felt that it helped them improve the management of relationships and their psychological well-being.

Debatin, Lovejoy, Horn & Hughes (2009) aimed to measure Facebook users' awareness of privacy issues and the potential benefits and risks of using Facebook. An online survey was used, with most Facebook users (91 per cent) already claiming to be aware of privacy issues on Facebook and that they restricted their profiles (77 per cent) by privacy settings. Furthermore, 69 per cent of respondents indicated that they had already changed their default privacy settings and about half reported that they restricted the profile so that 'only friends can see it. In addition, 10 per cent report that they accept 'anyone' as a friend, 37 per cent accept

people that they have 'heard about through others', and 52 per cent only accept people they know personally.

This study differs from previous ones in using an elite sample of 'lawyers, journalists, doctors and academics', as most of the previous studies used a sample of children, adolescents and university students. This study also differs from previous studies in its use information privacy management theory, which, according to the researchers' knowledge, is applied for the first time in a study for the Emirates and Middle East. At the geographical level, this study differs from previous studies in its focus on users of social networking sites in the Emirates and examines the privacy of their information, while other studies have focused on the USA and Europe.

Theoretical Background

This study relies on privacy management theory. The management theory of privacy (Petronio & Durham, 2008) focuses on the day-to-day decisions we make about how much information we disclose about ourselves to people and how much 'private' information we keep. This is based on five basic assumptions: The first is about 'private information' or information about things that are of great interest to a person; it influences the way we define who we are and the extent to which we disclose our information. The second is 'private boundaries', which is the distinction of crossing the line between public or private information, and the third assumption of 'control and ownership' suggests that we have a sense of complete possession of our private information, and in light of the concepts of control over our information and our ownership of it, we have a right to decide whether that information is to become publicly available or to remain hidden and the belief to disclose or conceal information is our decision because we 'own' the information. The theory holds that the individual should be in a position to control who is allowed to information (if anyone) to access this private information.

The fourth assumption is the 'rule-based management system'. This system provides a framework for understanding the decisions that people make regarding private information. The last assumption, which is 'management dialectics', focuses on the tensions between the forces that call for the disclosure of private information and those that call for its concealment. In other words, this part of the dialectic is similar to the theory of cognitive dissonance in that it involves the feeling of discomfort from the desire to possess two contradictory things simultaneously. Therefore, consideration must be given to how this information may be acquired, used and disseminated (Petronio, 1991). One of the criteria for disclosure and concealment of personal information according to this theory is related to the customs and traditions of privacy and openness in a particular culture, as privacy is defined as a societal value. If the prevailing cultural values in a society

were 'open', then the people who belong to this culture will follow openness more than secrecy (Habes, Elareshi, Ali, & Zian, 2022). The second criterion refers to the differences that may exist between men and women when defining privacy boundaries. Women need to feel confident about the people they choose, whereas men focus on appropriate situations. This difference is mainly related to the socialization of both men and women. The third relates to the idea that people make decisions related to disclosure based on their motives, which are related to the desire for the required change, according to the fluctuations in the interest-to-risk ratio. This can also occur when the motives of disclosure or concealment change, as in cases of divorce or the end of relationships between people, which affects the motives of disclosure or concealment.

The theory also identified two types of 'boundary coordination' that describe how we manage shared information, namely thick and thin, which are closed borders that allow little or no information to pass or be revealed, while thin borders are open. This allows all information to pass without restrictions. When an individual's personal information is protected by 'individual limits,' the permeability of these limits is constantly changing. This allows certain parts of the public to access parts of the information that belong to the individual. In sum, when private information is held by a single owner, the boundaries are said to be 'thick' because there is less likelihood of the information getting out into the public domain. Once information is shared with one or more people, the boundaries of the private information widen and become more permeable. Thus, it is considered weak or thin (Petronio & Durham, 2008). Based on this theory, the research team posed several key questions related to the benefits, risks and limitations of disclosing or concealing personal information on social media platforms.

Research Questions and Hypothesis:

RQ1: What is the nature of the information disclosed by users of social networking sites?

RQ2: Why users are disclosing or concealing information on social networking sites?

RQ3: What are the risks associated with disclosing social media information in the study sample?

RQ4: How do users protect their personal information and raise awareness of the risk of privacy violations on social networking sites?

H1: There are statistically significant differences between the sample demographics (gender, and educational qualification) and the level of awareness of voluntary disclosure benefits of personal information.

Method

This study aimed to investigate the level of the awareness of the Emirati public regarding the concept of privacy and the information security when using social media platforms. This study is based on the survey methodology, questionnaire is the most widely used tool in scientific research because it is a simple and quick way to collect data. It is considered the least expensive research tool in terms of time, effort, and money (Wimmer & Dominick, 2000).

This is considered one of the survey studies that tends to describe what is, interpreted and identified in the beliefs, attitudes and practices of individuals and groups through the collection and expression of information (Elareshi, Habes, Tahat, Ziani, and Salloum, 2022; Habes et al., 2021). The study population consists of the various categories and segments of Emirati society (doctors, engineers, journalists, lawyers and academics), government employees and retirees. It used an available sample of 300 respondents because it does not aim to generalize its results, but to take indications of the phenomenon. An online questionnaire was used by making it available on a link to direct the targeted sample (Aoun, Lagadec, and Habes, 2022). Out of 300 respondents only 218 questionnaires were valid and completed. As for the ethical consideration of conducting this research, on February 20th 2023, an ethical application was approved, which holds approval no (ERSC_20232446) by Research Ethics Review Board in the College of Graduate Studies.

The questionnaire consists of seven sections, including: demographic information; the most preferred social media; the type of data revealed by the sample; the sample's attitudes towards accepting or rejecting friend requests; motives for disclosing information; risks and benefits of disclosing information; and finally, the sample's protection mechanisms for their information. The sample attitudes were measured on Likert scale.

The paper used different statistics (SPSS) to answer the research question including: Arithmetic means and standard deviations, frequencies and percentages, multiple analysis of variance to test hypotheses, and Scheffe's test for post comparisons.

Validity and reliability

To ensure the apparent validity of the tool, the research team applied the questionnaire to an exploratory sample to ascertain the apparent validity, questions, the extent to which the questions and paragraphs were properly formulated to be understood by respondents and to consider the observations made by the respondents and benefit from them. The tool was also presented to several specialists who were professors in academic programs in media, sociology, education and economics. To verify the reliability of the tool through the coefficient

(Cronbach's alpha), it was found that the lowest value among the variables was 0.78 and the highest was 1.00. These values strongly indicated that the study tool had a high degree of use in data collection.

Results

This section provides a summary and analysis of the research results, including a description of the study sample's features, variables, and hypotheses testing. The results showed that 'Instagram' recorded the moderate level mean value among the statements being rated by the study sample; thus, it was ranked first, with a mean of (4.20), followed by Snapchat (4.07), TikTok (3.51) and Twitter (3.35), while Facebook was ranked last with a mean of (2.61).

Types of information that Emiratis discloses

It can be noticed from the data in Table 1.1 that "I do not share any of my personal information" was ranked first, with a percentage of 34.77 per cent, followed by 'birthday' (22.70 per cent), contact information, for example e-mail, phone number, address, home or house number, website' (13.79 per cent), information about 'gender' (12.64 per cent), 'marital status' (10.06 per cent) and lastly 'place of birth' (5.46 per cent).

Table 1.1: Frequencies and percentage about the Demographic sample characteristic.

Variable	Categories	Frequency	Percent
Gender	Male	44	20.2
	Female	174	79.8
Residence place	Abu Dhabi	168	77.1
	Dubai	8	3.7
	Sharjah	19	8.7
	Ajman	9	4.1
	Ras Al Khaimah	7	3.2
	Umm Al Quwain	1	0.5
	Fujairah	6	2.8
The profession	Student	50	22.9
	government sector	105	48.2

	private sector	12	5.5
	looking for a job	18	8.3
	Retired	15	6.9
	Other	18	8.3
Age	Less than 20 years	9	4.1
	21-40 years	125	57.3
	41-60 years	81	37.2
	More than 60 years	3	1.4
Educational level	High School	25	11.5
	diploma (college)	22	10.1
	Bachelor's	116	53.2
	Graduates studies	55	25.2
The number of hours of using and browsing social media platforms per day	less than an hour	7	3.2
	From an hour to 3 hours	89	40.8
	More than 3 hours and less than 8	95	43.6
	more than 8 hours	27	12.4
Total		218	100.0

Over one third (39 per cent) of the sample also did not like to share any of their 'educational information', followed by one quarter (25 per cent) who used to share information about their 'field of study major' and then information about their universities or schools (20 per cent). Finally, sharing information about their degrees was ranked last (17 per cent). Regarding sharing their work information, the data revealed that over two third (68 per cent) of the respondents did not share their work

information on their social media accounts, but about 14 per cent shared their information about their 'company name', following by 'workplace' (12.36 per cent), while information about their 'position at work' was ranked last (6.18 per cent). As to the way the sample registered their names on social media, the findings indicated that over one third (38 per cent) of the sample used their 'real name' in social media accounts, but a quarter (25 per cent) used their 'first name only', followed by using a 'fake name' (19 per cent), while 'nickname' was ranked last (17 per cent).

Regarding the type of image that the sample use on their social media account, over half (51 per cent) rated 'nature view' first, 'personal picture' (19 per cent) second, 'State symbol (leadership, flag, etc.)' (18 per cent) third, images of 'family only' (2 per cent) fourth, while 'additional photos of friends' was ranked last (0.92 per cent).

The findings of the study match with Azziz and Dakhane (2022)' findings which indicated that the UAE people consider their personal information on social media are sensitive and confidential, in particular, the financial and contact information. Per contra, the results inconsistent with Young and Wuan-Hass (2013) findings which revealed that individuals usually share large amount of information with others such as their addresses, phone numbers, photos, emails, and birthdays. As well the results are inconsistent with Shahid and Abdulla (2021)'s findings which indicated that most users put their real information on social media to the public. Also, the results of this study are in contrast to the results of Waters and Ackerman (2010), which indicated that users preferred to disclose information to distant friends than to close ones.

Friend requests

Data from Table 1.2 indicates that over two thirds of the sample (68 per cent) only accepted friend requests from people they personally knew, followed by accepting friend requests from people they might know through others (22 per cent), while some of the sample mentioned that they accepted friend requests from anyone who sent requests to them (10 per cent). Examining the previous findings indicated that the Emiratis imposed thick boundaries regarding sharing their personal information on social media and were keen to keep private information away from others. This result consisting with Saeri et al. (2014)'s findings which indicated that trust of people is the main factor of adding others to their friend lists on social media. Also, these findings match with Debatina (2009)'s findings, which indicated that users only accept people they know personally. However, the findings of this study do not match those of Shahid and Abdulla (2021), which showed that most users accept friend requests and invitations from unknown people.

Table 1.2: Accepting friend requests on social media

Fiend requests	Frequency	Percent
Only people I know personally	148	67.89
The people you might know through others	48	22.02
Anyone who sends a friend request	22	10.09
Total	218	100.00

Motivations of personal information disclosure

Table 1.3 shows the mean values and standard deviations of these motivations: **Information sharing:** It can be noted that phrase 2 “I reveal my information to share my experience with others” recorded in the moderate level, and ranked first with ($M = 2.68$), while phrase 1 “I reveal my information to share it and knowledge with others” ranked last, with ($M = 2.22$). The overall average of this variable is ($M = 2.44$), which indicated a moderate level of agreement among the sample. **Storing information:** This is storing information that means something to you in your life or that you often use. It can be noted that phrase 3 “To save and store personal ideas and photos” ranked first with an average of ($M = 2.55$), while phrase 1 “To keep my personal record” ranked last with an average of ($M = 2.28$). The overall assessment of this variable is moderate with averaged ($M = 2.41$). **Keeping up the trends and developments:** table shows that phrase 1 “I reveal my information because it’s hard to feel empathy for people unless you share your information” placed first and recorded low level among the sample ($M = 2.01$), while phrase 2 “I reveal my personal information because everyone else does it too” ranked last, with ($M = 1.88$). The overall assessment is low level with average of ($M = 1.93$).

Table 1.3: Motivations of personal information disclosure on social media

#	Statement	Mean	Standard deviation	Importance level
Information Sharing				
2	I reveal my information to share my experience with others	2.68	1.17	Moderate
3	I reveal my information to share them on a specific issue.	2.43	1.13	Moderate

1	I reveal my information to share them and knowledge with others	2.22	1.08	Low
Overall		2.44	0.96	Moderate
Storing information				
3	To save and store personal ideas and photos	2.55	1.18	Moderate
2	To store the important information from being forgotten	2.39	1.14	Moderate
1	To keep my personal record	2.28	1.10	Low
Overall		2.41	0.99	Moderate
Keeping up the trends and developments				
1	I reveal my information because it's hard to feel empathy for people unless you share your information through social media	2.01	0.99	Low
3	I reveal my information so that I don't stay out of time	1.89	1.01	Low
2	I reveal my personal information because everyone does it too.	1.88	1.00	Low
Overall		1.93	0.90	Low
Show off and seek popularity				
2	I reveal my information to show my abilities and potential	2.28	1.18	Low
3	I reveal my information to show off by marketing and advertising my activities	1.84	1.01	Low
1	I reveal my information to show that I'm famous and well-known	1.72	0.85	Low
Overall		1.95	0.87	Low
Leisure and entertainment				
1	I reveal my information because I enjoy doing it	1.95	1.05	Low
2	I reveal my information because doing so is a source of entertainment	1.93	1.08	Low

Overall		1.94	1.01	Low
Managing personal relationships				
5	I reveal my information to communicate with friends	2.66	1.24	Moderate
3	It serves as a place to meet between me and others	2.63	1.16	Moderate
1	I reveal my information to maintain a close relationship with others.	2.30	1.17	Low
2	I reveal my information through my accounts on social media	1.98	0.96	Low
4	I disclose my information to let people know about my current situation	1.86	0.90	Low
Overall		2.28	0.90	Low
Self-introduction				
1	I reveal my information to present myself in a realistic way to others	2.44	1.14	Moderate
3	I reveal my information to introduce my individual traits and characteristics	2.26	1.11	Low
2	I reveal my personal information to present my ideal self.	2.07	1.02	Low
Overall		2.26	1.00	Low
OVERALL		2.17	0.78	Moderate

Show off and demonstrate popularity: It can be noted that phrase 2 “I reveal my information to show my abilities and potential” placed first with an average of ($M=2.28$), while phrase 1 “I reveal my information to show that I’m famous and well-known” placed last with an average of ($M=1.72$). The overall assessment of this variable is low among the sample and averaged ($M= 1.95$). **Leisure and entertainment:** It can be noted that phrase 1 “I reveal my information because I enjoy doing it” came first with low average ($M=1.95$), awhile phrase 2 “I reveal my information because doing so is a source of entertainment” ranked last with an average of ($M=1.93$). The overall assessment of this variable averaged ($M=1.94$), which indicated low level of agreement among the sample.

Managing personal relationships: It can be noted that phrase 5 “I reveal my information to communicate with friends” placed first with an average of ($M=2.66$), while phrase 4 “I disclose my information to let

people know about my current situation” ranked last with an average of ($M=1.86$). The overall assessment of this variable averaged of ($M=2.28$), indicating low level of agreement among the respondents. Finally, **Self-introduction motivation**: It can be noted that phrase 1 “I reveal my information to present myself in a realistic way to others” came first with an average of ($M= 2.44$), while phrase 2 “I reveal my personal information to present my ideal self” ranked last with an average of ($M=2.07$). The overall assessment of this variable was low with an average of ($M= 2.26$). The findings of this study inconsistent with Waters and Ackerman (2010)’s finding which showed that improving the management of relationships and their psychological well-being are the most important motivations of disclosing information on social media

Table 1.4: The risks of an individual disclosing personal information

#	Statement	Mean	SD	Rank	Importance level
1	Disclosing my personal information to the wrong person.	1.84	0.84	1	moderate
3	The over-share information about ourselves or talk about ourselves	1.79	0.82	2	moderate
4	Unwanted progress on social media sites	1.78	0.79	3	moderate
5	stealth account tracking	1.75	0.83	4	moderate
2	Disclosure of private information at a bad time	1.74	0.78	5	moderate
8	Personal data stolen and misused by others	1.70	0.84	6	moderate
7	The gossip or rumors that are harmful	1.68	0.82	7	moderate
6	Online harassment	1.67	0.83	8	moderate
OVERALL		1.74	0.72	-	moderate

Based on Table 1.4 presents the values of means and standard deviations for the most prominent dangers of an individual disclosing his/her personal information on social networking sites, it noted that “Disclosing my personal information to the wrong person” was ranked first ($M=1.84$) as the most prominent risks of disclosing, while “Online harassment” was ranked last with ($M=1.67$). The overall risks level of disclosing personal information was moderate among the sample with average of ($M=1.74$). The finding of this study is consistent with Saeri et al. (2014)’s findings, which indicated that the sample reported experiencing negative Facebook effects, such as unwanted advances, stalking, harassment, gossip, damage, rumour or data theft. Also, the results of this study agreed with Faraj (2015)’s findings, which showed

that risk of self-disclosure on social media is lowered among users when they have high level of risk perception.

Based on Table 1.5 that presents the means and standard deviations for the most prominent benefits of disclosing personal information on social networking sites, it notes that statements 2 and 4 “validate our views” and “to enjoy self-expression” recorded a moderate mean value among the statements being rated by the study sample; thus, it was ranked first with a mean of ($M=1.86$), while statement 1 “Increased social control” was ranked last with a mean of ($M=1.63$). The overall assessment of this variable was rated as a mean of ($M=1.80$), suggesting a low level of agreement among the study sample. These results consistent with Waters and Ackerman (2010)’s findings, which indicated that users get closed to other new friends when sharing their information.

Table 1.5: The most prominent benefits of disclosing personal information

#	Statement	Mean	SD	Rank	Importance level
2	Validate our views	1.86	0.69	1	moderate
4	To enjoy self-expression	1.86	0.72	1	moderate
3	We become more confident and closer in our relationship with our partners	1.84	0.70	3	moderate
1	Increased social control	1.63	0.67	4	Low
OVERALL		1.80	0.58	-	moderate

Based on Table 1.6, which presents the values of means and standard deviations for mechanisms for protecting personal data on social media, we note that statements 3 and 7 (‘Protect my accounts on the social media from ads’ and ‘avoid accepting friend requests from strangers’) recorded a high mean value among the statements being rated by the study sample; thus, it was ranked first with a mean of 3.64, while statement 2 (‘I remove myself “your name” from the research results’) was ranked last with a mean of 3.27. The overall assessment of this variable was rated as a mean of 3.50, suggesting a moderate level of agreement in the study sample. These results agreed with Saeri et al. (2014) and Debatin et al. (2009)’ findings, which indicated that users restricted their profiles. But, these findings are not consistent with Katharine and Winter (2017), Young and Quan-Haase (2013), and Shahid and Abdulla (2021) who their findings indicated that users accept friend requests and invitations from unknown people, and they did not usually care to protect their accounts by not changing the initial privacy setting

for long time, besides, users of social media had little or no understanding of privacy settings.

Table 1.6: Mechanisms for protecting personal data

#	Statement	Mean	SD	Rank	Importance level
3	Protect my accounts on the social media from ads.	3.64	0.59	1	High
7	avoid accepting friend requests from strangers	3.64	0.61	1	High
5	Block and restrict photos from appearing, protect my albums	3.63	0.61	3	High
6	Avoid re-sharing posts of my embarrassed friends on my wall	3.52	0.67	4	High
1	Hide my friends list from a third party	3.43	0.69	5	moderate
4	Remove my content from Google	3.40	0.70	6	moderate
2	I remove myself “your name” from the research results	3.27	0.77	7	moderate
OVERALL		3.50	0.48	-	moderate

H1: There are statistically significant differences between the sample demographics (gender and educational qualification) and their level of awareness of voluntary disclosure benefits of their personal information.

Table 2.1: Three Way ANOVA of awareness the benefits of voluntary disclosure of information

Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Gender	0.008	1	0.008	0.014	0.906
Educational level	9.505	3	3.168	5.382	0.001
Error	121.864	207	0.589		
Total	139.460	217			

Table 2.1 shows no significant differences according to gender in the domain of ‘awareness of the benefits of the voluntary disclosure of

personal information’. This result disagrees with the results of Boyd and Hargitay (2010) which indicated that females are more wary than males of the privacy issues on social media. There are significant differences according to educational level in the domain of ‘awareness of the benefits of the voluntary disclosure of personal information’. Scheffé’s post-hoc test showed statistically significant differences according to educational level. There were significant differences in age groups in the domain of ‘awareness of the benefits of voluntary disclosure of personal information’. Finally, there were significant differences according to the number of hours spent using communication platforms in the domain of ‘awareness of the benefits of voluntary disclosure of personal information’.

Table (2.2) Scheffe’s test for multiple comparisons according to educational qualification

Level of education	Mean	diploma (college)	Bachelor's	Graduate studies
High School	1.93	0.968	0.981	0.055
diploma (college)	2.04	-	0.997	0.235
Bachelor's	2.00		-	0.007*
Graduate studies	2.44			-

Table 2.2 shows differences in awareness of the benefits of voluntary disclosure of personal information; there is a significant difference in the mean value between those with bachelor's and graduate studies, in favour of those with graduate studies.

Discussion

The findings of this study indicate that Emiratis actively seek to manage their privacy on social media. These results are sufficient to provide a clear perception that the Emirati community has an acceptable awareness when using social media platforms in their lives, and therefore, great knowledge and awareness of how to manage what is disclosed in their data or information on social media accounts. Considering numerous interpretations, this awareness is a ‘societal culture’ and not individual behaviour in Emirati society. The awareness of the importance of protecting personal data is the result of an extended and cumulative process in which various entities in the country participate in enhancing the concept of information security on social media platforms. It can be attributed to several possibilities, including the most prominent of these explanations being the efforts that the UAE has devoted years prior to smart transformation and government, which are in line with the national agenda that aims to become a UAE first to provide smart government services electronically

via mobile phones through the implementation of many initiatives, projects and services that encourage the public to use smart services efficiently and securely. The volume of spending on communications and information technology in the UAE reached AED 74.13 billion (\$20.2 billion) in 2023, compared to AED 71.84 billion (\$19.5 billion) in 2022, a growth of 3.2%, according to the International Data Corporation (Al-Arabi, 2023). This amount of spending is an indication of the official interest in smart transformation and thus reflects people's dealings and enhances confidence in the use of smart applications in the services provided by the government.

Another possible reason for the level of awareness of the protection of information privacy for Emiratis may be related to the thorough and effective awareness and media campaigns implemented by competent authorities in the Emirates years ago to promote a safe and reliable digital environment in the UAE. These campaigns, such as the 'Safer the Internet' campaign, consumer protection campaigns in digital transactions, 'Cyber Pulse' initiatives, 'UAE Ambassadors for Cybersecurity', 'Cyber security is everyone's responsibility', 'Salem Awareness Initiative' and other campaigns and initiatives aimed at providing a safe electronic environment for all internet users, contribute to the rising generation on such initiatives. All these efforts contributed to creating a community culture that can raise public awareness of the requirements for using the digital environment and smart applications.

In addition, the deterrent UAE legislation and laws related to cybercrime and privacy violations may have contributed to strengthening the responsibilities of citizens when using social media platforms and sharing personal data on those platforms. Finally, among the possible explanations for this high level of awareness, the UAE Ministry of Education curricula may include topics related to the digital environment and digital knowledge management, as well as the expansion witnessed by many Emirati national universities in the development of cybersecurity specialization and the increasing demand for it.

Limitations and future research

It is important to examine the concepts of privacy and information security for the public on social media in the UAE (Emirates). Social media is a widely used platform in the Emirates; understanding how the public perceives and values privacy and information security is crucial for ensuring the responsible use of these platforms.

There are some limitations to this study that suggest opportunities for future research. One such limitation is the lack of specific data on the Emirati public's level of awareness and behaviour regarding privacy and information security on social media. Although studies have suggested a growing awareness and concern among social media users in the UAE, it is difficult to draw definitive conclusions without more detailed

information about specific behaviours and attitudes. Future studies should use surveys, focus groups or other research methods to gather more specific data on these topics. Another limitation was the focus on Emirati social media users, who may not be representative of the broader UAE population. It is possible that non-users of social media, or individuals who use social media less frequently, may have different attitudes and behaviours regarding privacy and information security. Future studies could explore these differences and examine whether specific demographic factors influence attitudes and behaviours. Finally, there is a need for research on the effectiveness of educational and awareness campaigns aimed at promoting privacy and information security on social media in the UAE. While such campaigns are an important step towards addressing the challenges associated with social media use, their effectiveness in changing behaviours and improving outcomes is unclear. Future studies could use experimental or quasi-experimental designs to assess the impact of these campaigns on specific outcomes, such as knowledge, attitudes and behaviours.

Recommendation

Amid the increasing growth of new academic programs related to cybersecurity, it would be a good moment for inviting researchers from multidisciplinary background to conduct joint research in some unexplored issues. Also, the results of this study may benefit not only decision-makers in the UAE, but also graduate students in Digital media majors. Here, a group of academics can also develop a curriculum for digital awareness, which might be a compulsory requirement for all university students to enhance the concept of privacy awareness in light of the increase in violations. Thus, the study would recommend that education and awareness campaigns can help raise awareness about the risks and best practices for privacy and information security on social media.

Conclusion

This study focuses on the day-to-day decisions we make about how much information we disclose about ourselves to people and how much 'private' information we keep. This assumes of control and ownership suggests that we have a sense of complete possession of our private information, and in light of the concepts of control over our information and our ownership of it, we have a right to decide whether that information is to become publicly available or to remain hidden and the belief to disclose or conceal information is our decision because we 'own' the information.

Emiratis in this study did not disclosed a large amount of information that they usually share with others, over 61 per cent of them did not use their real names on social media accounts, but prefer to use fake names, nicknames, or only the first name. The same as well when using photos,

the over majority of the Emiratis (81 per cent) did not upload their personal photos on their accounts, but they uploaded other types of photos other than their personal. As for their personal information like education, work, birthday, contact information, etc. Emiratis in this study agreed that personal information should be private and confidential on social media, and the showed that they were worried about protecting their privacy on social media, so this is why the overwhelming majority (90 per cent) only accept friend requests from people they know either personally or through others.

It can be said that there is an acceptable level among Emiratis regarding their awareness of the nature of the risks arising from their disclosure of their information on social media, and it is the same level regarding their awareness of the most important benefits that result from this disclosure.

Protecting their accounts from ads, avoid accepting friend requests from strangers and restricting their photos from appearing are the most mechanisms that Emiratis do for protecting their personal data on social media.

Funding Acknowledgements:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Bibliography

1. Al Amir, S. (2022). More than 25,000 cybercrimes reported last year, say Dubai Police, retrieved on 26th December 2022 from <https://www.thenationalnews.com/uae/2022/08/24/more-than-25000-cybercrimes-reported-last-year-say-dubai-police/>
2. Al Olaimat, Farhan, Mohammed Habes, Al Hadeed, Ali Yahya, and Marcelle Issa Al Jwaniat. 2022. "Reputation Management through Social Networking Platforms for PR Purposes: A SEM-Based Study in the Jordan." *Frontiers in Communication* 11(3):247.
3. AlArabi, Y. (2023). 74 billion dirhams spending on communications and information technology in the UAE, retrieved on 21st March 2023 from <https://www.alittihad.ae/news>
4. Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing Company.
5. Aoun, Charbel Geryes, Loic Lagadec, and Mohammad Habes. 2022. "An Extended Modeling Approach for Marine/Deep-Sea Observatory." Pp. 502–14 in *International Conference on Advanced Machine Learning Technologies and Applications*. Springer.
6. Azzi, A., & Dakhane, S. (2022). Social Media and Privacy in the UAE: A Survey Research, *University of Sharjah Journal for Humanities & Social Sciences*, (19) 2, pp.569-604.
7. Blumberg, Daniel M., Luciano Giromini, and Laura B. Jacobson. 2016. "Impact of Police Academy Training on Recruits' Integrity." *Police Quarterly* 19(1):63–86. doi: 10.1177/1098611115608322.

8. Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday Journal* 15 (8).
9. Cohen, S. (2016). Privacy risk with social media. available at https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html
10. Davison, W. P. (1983). The third – person effect in communication. *Public opinion quarterly*, 47, 1-15.
11. Debatin, B., Lovejoy, J., Kathrin Horn, A., & Hughes, B. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, 38-108
12. Elareshi, M., Habes, M., Tahat, K., Ziani, A., & Salloum, S. (2022). Factors affecting social TV acceptance among generation Z in Jordan. *Acta Psychologica journal* 230, 103730.
13. Faraj, P. (2015). The culture of privacy through social networking sites between the advantages and risks of self-disclosure: A study in the attitudes of the Egyptian public. *The Egyptian Journal of Public Opinion Research*, 14 (1).
14. Global Media Insight Report. (2022). More than 32 million social media users in the UAE. retrieved on December 18th 2022 from <https://www.globalmediainsight.com/blog/uae-social-media-statistics/>
15. Gordon, A., Loeb, M., Lucyshyn, W., & Lei Zhou. L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb Model. *Journal of Information Security* 6(1),2430.
16. Habes, M., Ali, S., & Pasha, S. (2021). Statistical package for social sciences acceptance in quantitative research: From the technology acceptance model's perspective." *FWU Journal of Social Sciences* 15(4):34–46. doi: <http://doi.org/10.51709/19951272/Winter-2021/3> Statistical
17. Habes, M., Elareshi, M., Ali, S., & Ziani. 92022). Analyzing the portrayals of child sexual abuse of Urdu newspapers in developing countries." *Pertanika Journal of Social Science and Humanitiesopen* 2.
18. Katharine, S. & Winter, L. (2017). Social Media Users' Legal Consciousness About Privacy. *Social Media + Society journal*, 3 (1),1-14.
19. Khan, Z. Reza., Rakhman, S. & Bangera, A. (2016). Who stole me? Identity Theft on social media in the UAE', 4th Global Conference on Business and Social Sciences, Global Academy of Training and Research, Dubai, UAE.
20. MENA Herald Website. (2016). Norton Reveals More than 2.5 Million UAE Consumers Were Affected by Cybercrime in the Last Year. Retrieved on 26th December 2022 from <https://www.menaherald.com/en/tech/information-technology/norton-reveals-more-25-million-uae-consumers-were-affected-cybercrime>
21. Petronio, S (1991). Communication boundary management: A theoretical model of managing disclosure of private information between married couples. *Communication Theory* 1 (4), 311–335.
22. Petronio, S., & Durham, W.T. (2008). Communication privacy management theory. In L.A. Baxter & D.O. Braithwaite (Eds.), *Engaging theories in interpersonal communication: Multiple perspectives* (pp. 309-322). Thousand Oaks, CA: Sage.
23. Saeri, A., Ogilvie, C., La Macchia, S., Smith, J., & Louis, W. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm

- focus and the theory of planned behavior. *The Journal of Social Psychology* 154(4).
24. Shahid, A., & Abdulla, U. (2021). Privacy threats on social networking websites, *Foundation University Journal of Engineering and Applied Sciences* 2 (1), Available at: www.researchgate.net.
 25. Tahat, D., Elareshi, M., Tahat, K., Jwaniat, M., Habes, M., & Ziani, A. (2022). News media and political participation in the Middle East: Jordan as an example. *The International Arab Conference on Information Technology (ACIT)*, Abu Dhabi, UAE. pp. 1-8, doi: 10.1109/ACIT57182.2022.9994199
 26. Wang, S., Habes, M., & Li, M. (2022). Motivations influencing Alipay users to participate in the Ant Forest Campaign: An empirical study. *International Journal of Environmental Research and Public Health* 19(24):17034.
 27. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
 28. Waters, S., & Ackerman, J. (2011). Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure. *Journal of Computer-Mediated Communication* 17(1), 101-115.
 29. Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum
 30. Wimmer, R. D., & Dominick, J. R. (2000). *Mass media research: an introduction*, (6th Ed.). Belmont, CA: Wadsworth Publishing Company.
 31. Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479-50
 32. Zogheib, S. (2009). *Research methods and statistical uses in media studies*. Cairo: The Egyptian Lebanese House.