Students' Perception of Social Media Privacy in UAE: Case Study of the University of Sharjah

Reem Almarmoom[*]

Supervised by: Dr.Khaled Zamoum[**]

Abstract:

This study aimed to assess the social media privacy perception of students in the University of Sharjah (UOS). This study used a quantitative method. 146 students voluntarily completed an online survey in english. The findings revealed two major results: A figure of 91% of students were active on social media platforms, with Snapchat and Instagram being the most popular choices. However, it was concerning that 92% of these studentsdo not fully comprehend and do not read the terms and conditions of these platforms, pointing out a gap in awareness and digital literacy. Students expressed concerns about privacy breaches, with identity theft ranking as the top worry. The United Arab Emirates' (UAE) stringent legal framework imposing imprisonment and fines for cybercrimes was seen as a defensive factor. It is suggested by this study that increasing digital literacy among students is an important aspect to take into consideration, and that education in this area is imperative.

Keywords: Social Media, Privacy, Legislation, UAE Students, Communication

Introduction

The following study emphasizes the effect of social media privacy on students. In this era of digitalization, social media plays a pivotal role in our daily lives. Young adults have become dependent on social media for different reasons. It facilitates human lives in numerous ways. However, deficiency in comprehensive privacy measures includes the possibility of exposing personal data, making students vulnerable to identity theft, cyberbullying, and virtualharassment. As most of the social media users are students, this study aims to evaluate

[*] Postgraduate student College of Communication at the University of Sharjah, UAE

[**] Associate professor College of Communication at University of Sharjah, UAE

the impacts of social media privacy on students and the UAE's legal protection.

Importance of the study

Importance of this study mainly focuses on exploring the perception of social media privacy on the students in UAE. This study addresses crucial concerns in the modern digital landscape. In the era where social media is vital in student’s lives, recognising the implications of inadequate privacy measures becomes essential. The study uncovers the possible risks which students can face including, identity theft and data mining. It highlights the necessity of informed digital practices. Furthermore, shedding light on the privacy setting and potential legal ramification in this study contributes towards increasing awareness among students. Incorporation of survey results delivers practical dimensions. It provides significant evidence towards behaviour and attitudes of the students’. Finally the findings offer vital insights for educational institutions, students and policymakers. Therefore it guides the development of significant strategies, educational programs and legal framework to protect digital privacy in the UAE.

Literature Review The Definition of Privacy

The term 'Privacy' defines an individual's right to protect and control their personal information, private spaces, and activities (Acquisti et al., 2020). As mentioned in the report of the United Nations High Commissioner for Human Rights(United Nations, 2018), right to privacy is a freedom from unwarranted control and disclosure over the personal information of the citizen (United Nations, 2018).It contributes in protecting private life, home, family from the unlawful consequences. It also highlights surveillance protection and data control. It covers a wide perspective of freedom and personal autonomy from intrusion. It ensures these aspects of people's lives remain free from unauthorized access, public scrutiny, and intrusion. As stated in an article of A Contextual Approach to Information Privacy Research (Wu et al., 2019), privacy in the context of social media reflects the individual's right to protect and control their personal information, communication, and different activities from unauthorized access, utilization, and disclosure. It includes the protection of sensitive data, like location, contact details, online interactions, and preferences, from being exploited for commercial purposes, potential misuse, or targeted advertising by malicious actors. Multiple digital platforms are established on algorithmic processing, excessive collection, and financial exploitation of personal data of the users; for instance, Meta, YouTube, Instagram, Tiktok, X, LinkedIn, etc.

However, the extraordinary and rapid development of social media has provided online platforms with proficient access and encouragement into users' lives. Social networking organizations acquire sensitive data regarding activities, personal characteristics, preferences, political views, online behavior, and purchasing habits of the users. These data are utilized in multiple cases to algorithmically lead user participation and sell behavioral advertising (Jain et al., 2021). Often, these have discriminatory and distortive impacts. Although every social media organization has its typical privacy policies, sometimes they may be inadequate to safeguard the sensitive information of their users. Different websites and digital platforms publish privacy policies that are disclaimers. The most critical thing related to this is that often those policies are more likely to be vague and difficult to interpret with 'full of loopholes'. They might be subject to 'unilateral' transformation by those platforms and impossible or challenging to enforce for the injured users.

Social media privacy policies mainly encompass i) a 'controller for data processing,' ii) personal data transmission, iii) data mining, iv) data breaches, and v) fake information (Jain et al., 2021).

Over the past several years or more than a decade, several organizations have been putting effort into safeguarding the privacy of social media users' information (Jain et al., 2021). Digital platforms play a significant role in shaping the privacy experiences of their users with their determination in the collection, sharing, and storage of users' data. Therefore, it has become important for those platforms to implement comprehensive privacy policies and practices that empower users to control their information visibility and effectively manage their online presence (Epic, 2023). This asks for digital literacy and privacy awareness among the users to safeguard themselves and make informed decisions about the thing they share and their preferred audiences.

The Impact of Social Media Privacy on Students

The most popular reason to use social media is to share images and videos along with personal data (Oliveira et al., 2020). It includes the threat of using those data against the users.

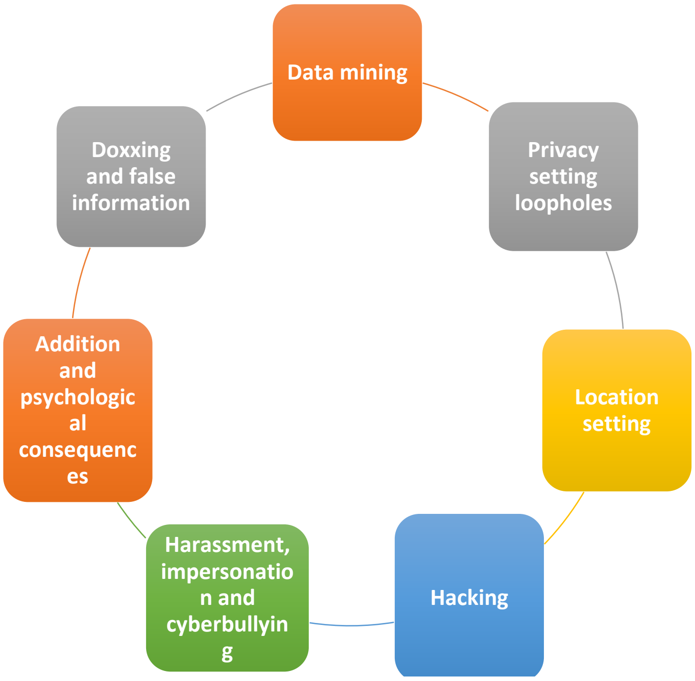
Data mining
Privacy setting loopholes
Location setting
Hacking
Harassment, impersonatio n and cyberbullyin g
Addition and psychologic al consequenc es
Doxxing and false information

Figure 1: Common social media privacy issues and their impacts on students

(Source: Authors' processing)

Data Mining

It is already mentioned that data is the foundation of social media platforms. Their tailored services, market analysis, business models, served advertisements, etc, are based on user information. Sometimes, personal data are referred to as the goldmines for social media platforms. This comprises the risk of data mining. Providing too much personal information and posting images, likes, and dislikes can draw pictures of the characteristics of the user. After giving consent to the digital platforms, the personal information of the users completely belongs to them, and they can use it according to their needs. It is reported in the 'Cambridge Analytica scandal' that it influences the opinions of the users according to their likes and dislikes. In this case, the personal data of millions of Meta users were misused (theguardian.com, 2019).

Therefore, the risk of data mining is serious for students. Sharing excessive data can make the students lose their control over it. This includes the consequences where their data can be used for different purposes that they may not approve or in such unexpected ways.

Models of privacy protection

Thecomprehensive legislative model: The comprehensive legislative model is a privacy protection approach that is significantly involved with the establishment of encompassing and thorough laws and regulations to protect the privacy rights of individuals in the digital era. Under this model, government enforcement legislation sets a clear standard in processing, collecting and disseminating personal information. This aims in delivering a uniform and robust infrastructure which is applicable across several sectors. It guarantees accountability and consistency in handling the sensitive data. Key components also include defining the rights of individuals in specifying the lawful grounds for instituting regulatory bodies in overseeing the compliance. General Data protection regulation in the European Union exemplifies the complete legislative model (Cipolletta et al., 2020). It also serves as a significant benchmark for universal privacy standards and highlights the importance of user consent and stringent penalties in case of non-compliance.

The sectoral model: Sectoral model of privacy protection is a targeted approach that highlights regulations towards particular sectors. It recognises several factors that contribute to differentiating several sectors that can face privacy related challenges. Rather than implementing universal rules, this model envelopes a sector specific privacy guidelines and laws. Main aim of this model is to address the unique risks and intricacies that are associated with data handling in several domains. For example, the Health insurance accountability and probability act in the United States is a significant example of a sectoral model. It focuses significantly on protecting the security and privacy of health information. This model recognizes the diversified sectors (Jain, Sahoo & Kaubiyal., 2021). It aligns with the specified requirements and characteristics of each industry in guaranteeing significant protection of individual personal data.

The self Legislative model: The self legislative model mainly observed in social media platforms. In this model responsibility for enforcing and crafting privacy standards rests with the platform itself. Social media companies design privacy policies, user agreements and several service terms that users need to adhere to while using the platform. User consent towards these terms grants these platforms to possess, collect and share the personal information within the bounds that is specified by the policies of the platforms. For instance, Data use policy in Facebook and privacy policy of Instagram. This model offers flexibility for several platforms and helps in adapting quickly to several evolving technologies (Ahmed, 2020). It also increases concerns about significant conflicts among the profit motives of platforms and privacy rights of users. Users get inspired in navigating and adjusting the platform specific privacy setting to align with the comfort levels and preferences.

Model of protecting user privacy within social media platforms: This kind of model depends on individuals to protect their own privacy in social media platforms. It helps users to actively safeguard and manage their personal information. In this user centric model, individuals are encouraged in taking active measures to control the visibility of data. This kind of model contributes to adjusting privacy settings and exercising discretion in sharing personal information. Social media platforms also provides its users with a range of privacy controls Moreover it allows in customising the privacy setting on the social media to set who can access their content, view their profiles and interact with them (Whitehill et al., 2020). This model highlights digital literacy and user education. It urges individuals to become aware about potential risks and results in sharing particular information online.

Privacy Setting Loopholes

Most of the social media platforms have published their updated privacy policies. Still, they do not always assure privacy (Epic, 2023). It allows the group members in the closed group to share anything posted by other members in another group. This is how friends of friends can see that content that was not intended. Therefore, a lack of stringent policies among other users can create some circumstances that were not expected.

It is reported that teenagers, who are mainly students, share too much information regarding themselves on social media platforms more than before (Cipolletta et al., 2020). X use by teens also has increased in the last ten years (Whitehill et al., 2020). For instance, several digital platforms have stated that they utilize their user's information ethically, but still, there are causes for concern. Meta also claimed that they collected call records along with the messaging history of their Android users since 2017 to improve their messaging service without their concern (Vomiero, 2019).

Location Setting

It is very important to focus on location settings during accessing mobile applications and social media sites, as the location of the users might be a valuable piece of information. It can profoundly impact the students. Though sharing current or frequent locations helps the students to connect with friends and discover nearby places and local businesses, it also raises awareness in several ways. Sharing real-time locations may pose a threat to the personal safety of the students (Wilmott, 2020). It may allow others to track their movements and know their exact locations, which can make them vulnerable to theft or physical harm. Broadcast location information may attract unwanted attention from strangers, cyber stalkers, or acquaintances if their whereabouts are constantly accessible. Moreover, a combination of such data with other personal information can also be used for data mining and profiling that may lead to tailored advertisements and student preference manipulation.

Hacking

It is found that students mainly post pictures and videos of themselves, their school's name, present city or town, email address, phone number, birth date, real name, interests, and relationship status (Cipolletta et al., 2020). Access to such personal information allows hackers to collect information from the social media profiles of the students and utilize them to break the accounts. It is one of the easy tricks to post a picture of your favorite pet and use its name as a password. Thus, hacking the accounts of the students is relatively easier. Moreover, pretexting and phishing are also reported to be the most popular social engineering attacks after obtaining a better understanding of the user (Eckert & Metzger-Riftkin, 2020). Also, spreading viruses and malware through sending a link from a hacked account on social media is higher than email phishing, as people believe in messages sent by friends.

Harassment and Impersonation

Harassment can be performed on social media without hacking the profile. It mainly includes sending threatening messages to classmates and ex-partners for blitzing them with inadequate comments (Abarna et al., 2022). It may result in a privacy nightmare, particularly if the messages have been sent from their accounts after hacking.

Doxing and False Information

The frequency of spreading propaganda and misinformation on social media platforms is higher. Students can face roles that may provoke unnecessary discussion intentionally and manipulate the motions (Eckert & Metzger-Riftkin, 2020). Therefore, it is important to cross-check the news if they seem suspicious.

Legal Actions in the UAE When it Comes to Privacy

UAE has laws related to online activities and social media privacy. The country offers opportunities to use social media platforms for different purposes but has set up rules that should be followed while using such platforms. Cybercrime Law which is also known as Federal Decree-Law No. 34 of 2021, deals with cybercrime and combats rumors to provide digital security and cyber safety (UAE, 2023). It addresses misuse and abuse of online technologies. It also aims to protect databases and websites of the government in UAE from online crimes, electronic fraud, and fake news. The law ensures penalties for using online platforms to hack and attack. It identifies theft and unauthorized access to networks and computer systems.

Federal Law No. 5 of 2012 and its article 21 under Cyber Crime Law Federal Law No. 3 of 1987 from UAE Penal Code and 2002 Copyright law claims it as an offense when a person clicks photographs of another person by not taking his or her consent and publishes them on social media.

Social Media Laws of UAE have been strongly set by the authority. It has been claimed that in case of violation of any of these laws, individuals might have to pay a fine of up to AED 1 million (UAE, 2022). Even imprisonment will also be a punishment side by side. One survey has revealed that many residents have indicated their worry related to cyber-attacks and Hacking.

Article 35 under UAE Cyber Crime Law claims penalties and imprisonment for offensive and insulting posts by a user on social media. The duration of imprisonment will be seven years, and penalties will be between AED 250,000 to AED 1 million (Mehta, 2023). Cyber Crime Laws of the UAE ensure safe communication across all media channels.

Five years imprisonment and penalties from Dh 250,000 to Dh 1 million are the punishment for posting any content harmful to the privacy of children and women. UAE's federal public prosecution has launched the "My Safe Society" app. The public can report cybercrime by dialing 999 or having access to Aman Service by Abu Dhabi Police (UAE, 2023). It can be reported online at www.ecrime.ae, 80012. Individuals can also get help from the toll-free number 116111 of the Interior Ministry. Dubai Police maintain an eCrime website to take legal action against any online abusive activities. In the country, therefore, individuals need to follow social media laws. If a person accepts paid advertisements or becomes a social media influencer, then he or she must obtain a license registered from the National Media Council.

The UAE has constantly taken a tough stance against online harassment and cyberbullying. Laws related to cybercrime in the UAE have given powers to the court to confiscate software, devices, and contents used in conducting a crime by using online platforms. According to Ahmed (2020), in UAE, the person who conducts cyberbullying faces a fine of up to Dh 150,000 and gets a six-month jail sentence.

The new law against cyberbullying came into effect on 2nd January 2022. The President of the country has approved wide-ranging reforms in the legal frameworks, and over 40 laws have been included in the recent changes made to these legal frameworks. In the 50-year history of the nation, such legal reform represents the largest legal transformation to address and prevent social media harassment and privacy concerns.

Privacy Issues Encountered in Social Media Platforms

In social media platforms, privacy issues are becoming a major concern that needs to be addressed and prevented. Some of the privacy issues encountered in social media platforms are,

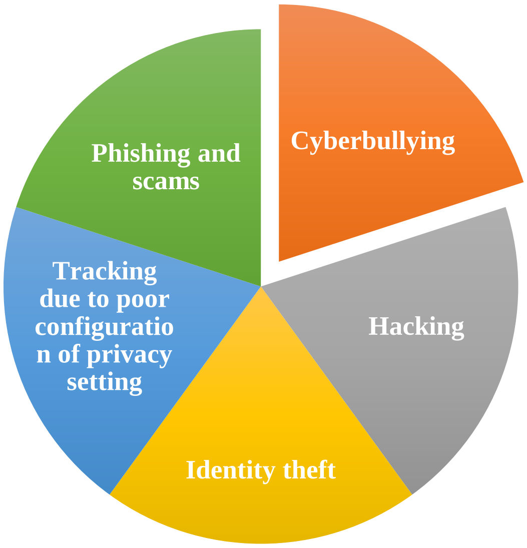

Figure 2: Some of the privacy issues encountered in the social media platforms

(Source: Authors' processing)

The youth population especially is suffering from social media privacy as they are emotionally immature and unaware of online harassment threats. As stated by Swenson-Lepper and Kerby (2019), cyberbullying and harassment are some of the major privacy issues encountered in social media. Students who are at a young age face psychological distress and safety risks due to cyberbullying. A study has reflected a high rate of cyberbullying among university students in the UAE due to the use of social media platforms.

Criminals always target young people as they do not have the proper sense of right and wrong. As per Abaido (2019), data collected from a survey of 200 students highlighted that 91% of respondents have confirmed that in UAE, there is a high presence of cyberbullying on social media. The rate of cyberbullying acts particularly on Meta (38%) and Instagram (55.5%). The UAE indeed maintains a strong unit in police departments against cybercrime, but more encouragement is needed for victims to report the issues they are facing.

Identity Theft

Identity theft is one crucial issue that hampers privacy on social media. It steals private information by using technology-based methods. After stealing personal information, the offender commits crimes to impersonate the victim. As mentioned by Al Shamsi (2019), an interview has been arranged by the Ministry of Education to learn about the perspectives of trainers and students on identity theft. They have indicated identity theft as a heavy threat to privacy. Therefore, the Ministry is providing a Cybersecurity Awareness Program at government preliminary schools in UAE for students in grade 4. They have targeted students aged between 8 to 10 years, as most of the emotional vulnerabilities occur in this stage. It is because of the unawareness of the children that they share sensitive private information on social media pages which exposes them to the threat of identity theft. Offenders use the private information of the victims and steal their identity to conduct offensive activities under the name of the victim. Such privacy issue is causing a high level of depression and a suicidal tendency among youth.

Critique of their previous studies

The previous studies of social media privacy among college students specifically in the gulf or Arab region, laid a significant foundation in understanding several aspects of this study. However effective gaps in the scholarship also exist that warrants various further discoveries. Present studies show a lack of comprehensive examination about the legal framework that lowers the effectiveness in protecting the privacy rights of students in the Gulf region specifically in the UAE. Some students touch upon the privacy concerns that impact significantly on the students. Therefore there is a necessity for more advanced analysis of present legal structure and their practical implications. Furthermore the research also focuses primarily on the behavioural aspects of the students like awareness, actions and concerns which are related to social media privacy. However there is a lack of research investigation that significantly stimulates the legislative measures and their alignment with the international standards. Moreover, methods adopted in previous study significantly depend on self reported data and surveys. Therefore it lacks in the depth qualitative insights. A pilot or exploratory study can be significant in refining the research question and can help in developing more targeted questionnaires. Absence of such preliminary investigation can lead towards overlooking the vital dimensions of social media privacy that are pertinent to Arav College students.

In order to address the gap, the research study aims to conduct a complete examination of the legal framework. It incorporates significant insights from a pilot study to refine the research tool. Delving within the experience of Emeriti college students and Gulf counterparts the study intends to contribute towards a more complete understanding about social media privacy. Understanding includes encompassing institutional, legal and individual perspectives.

Theoretical Framework

The theory of Communication Privacy Management (CPM) explains how disclosure and privacy can be managed based on the involvement of others. CPM theory was developed by Petronio in 1991 to provide a better understanding of how individuals manage their private information. The CPM theory was originally conceived as a model for interpersonal communication since computer-mediated communication has become increasingly popular, research on the CPM theory has expanded (Hooper, 2017). This theory explains how people decide whether to disclose their private information or information obtained from others. In addition to the effects of being a confidant, the theory also explores the effects that privacy turbulence can have on relationships (Child & Petronio, n.d.). Five principles underlie this theory: Privacy Boundaries, Private Information, Control and Ownership, Rule-based Management, and Dialectics of Privacy Management (Petronio, 2002).

The first principle is privacy boundaries, which can either be personal or collective and refer to metaphorical boundaries between public and private information. As a rule, personal boundaries refer to information that is personal to an individual, while collective boundaries refer to information that is private to a group, such as an organization or a family. According to the second principle, disclosing private information is the same as disclosing personal information.

CPM argues that disclosure and intimacy have different purposes since intimacy merely constitutes the act of disclosing private information. In the third principle, control and ownership, individuals own their private information, and they exercise control over it by disclosing and concealing it. To understand the management of privacy in communication, the fourth principle, a rule-based management system, involves the construction of two interrelated levels: the personal level and the collective level. Under this principle, three management practices are applied: privacy rules, boundary coordination, and boundary turbulence. There is a tension between private secrecy and public disclosure according to the fifth principle: the dialectic of privacy. Dialectical tension can be seen in how a person decides what to divulge or not to divulge (Waters & Ackerman, 2011).

College students use social media to communicate with each other and manage their personal information, according to a study by Yang et al. (2016) under the title examined the relationship between privacy concerns and social media usage, students believe they own their personal information and have the right to control how it is accessed, shared, and used, according to the theory of CPM. This motivates them to regulate the access and sharing of their information on X

(Yang et al., 2016). A recent study examined how Instagram users manage their privacy, finding that the theory provides a "mind map" that explains how people decide to share their personal information (Aini & Alamiyah, 2022). This theory is related to the research topic in that social media users are responsible for ensuring that they're sharing appropriate information with the audience and not violating their privacy.

Digital media platforms that are large and powerful tend to run on their own. A key aspect of the social web has been the rise of the platform as the dominant infrastructure and economic model. These connections between social media platforms and interfaces with other websites and data flows were created to achieve this rise. By leveraging the Internet as an economic and cultural platform, a handful of companies have been able to diversify their services. Media and cultural environments now operate under a platform paradigm that extends beyond the internet and social media.

According to Van Dijck and Poell (Dijck & Poell, 2013), media logic is a set of principles, or a set of theoretical rationality cultivated by media institutions. It penetrates and dominates all public domains. Social media logic is defined by four principles: programmability, popularity, connectivity, and datafication. In particular, the datafication principle is relevant to content creators and platform providers. The purpose of datafication is to collect and sort digital records of cultural practices and cultural international relations to analyze, aggregate, and deploy these records for strategic purposes. Social media companies, advertisers, and third-party intermediaries share these data not only through a single platform but through a far more extensive ecosystem (Baym et al., 2021).

Research Problem

The research problem discusses how students at the UOS perceive privacy concerns on social media, their awareness of potential privacy risks, and their understanding of the legal security announced by social media platforms.

Research Questions

RQ1. How do the students at the UOS perceive social media privacy?

RQ2. Are students aware of the risks of violating privacy?

RQ3. How do students perceive the effects of violating privacy on their private lives?

RQ4. Do the students know the UAE's legislation regarding the protection of social media privacy? And do they respect it in their usage?

Research Method

In this study, data was collected and analyzed using a quantitative method. This research has used the survey questionnaire method to collect primary quantitative data. The method includes a survey asking social media users about privacy concerns related to social media use. Collecting data from the students of Sharjah University makes the study very close to the case study. The survey captured social media usage, users' awareness of online information, and awareness of the legal implications of sharing information.

Population and Sampling

The main target group of the study is students between the ages of 18 and 24. The target group is intended to represent young adults who are active on social media platforms. A sample of 200 male and female students from the University of Sharjah were randomly selected to participate in the study. Participants received a link to the survey to answer the questions from March 20, 2023, till June 13, 2023, the total number of students who responded is 146.

Results1: Demographic and Personal Information

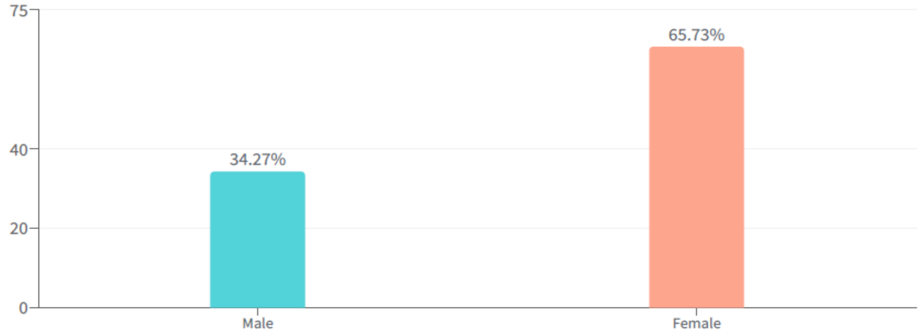

Figure 3: Research method used in researcher data

(Source: Authors' processing)

In the context of the demographic profile of the respondents, information about respondents has shown that among 143 respondents who have answered, there are 34.27% of respondents which are male, and the other 65.73% of respondents are female. Therefore, among the respondents the majority are female, and the remaining respondents are male who have given the responses. It was required to have the response of 146 respondents; however, 3 respondents skipped the questions as they were unwilling to respond to their gender.

Furthermore, the information about the respondents' age in the demographic information context has shown that responses have been given by 127 respondents and 8 respondents have skipped the question regarding their age specification. It is, therefore, found that most of the respondents that are 45.67% of respondents are aged between 20-22 years of age, whereas 43.31% of respondents are aged between 22-24 years. And, remaining 11.02% of respondents are aged between 18-20 years.

On the other hand, among 131 respondents who have given responses regarding their educational qualifications, it is observed that 58.78% of the respondents are undergraduates, and the remaining 41.22% of respondents are postgraduate. However, 3 respondents have not given responses regarding their educational qualifications.

On the other hand, being asked whether they own and operate at least one social media account, 90.08% of the respondents responded that they have at least one social media account. Only, 9.92% of respondents have stated that they do not have any social media account.

It further asked the respondents how long they have been using social media platforms. In that context, 53.08% of the respondents have stated that they have been using social media platforms for more than 6 years. 36.92% of the respondents have been using social media for 5-6 years, whereas 7.69% of the respondents have been using social media for 3-4 years. And only 1.54% of the respondents have been using social media for 6-12 months and the remaining 0.77% have been using it for 1-2 years.

Moreover, regarding respondent's responses regarding which social media platform they are most active on, it is seen that 91.54% of respondents use Instagram and Snapchat social media accounts. 76.15% of the respondents use X, 51.54% of respondents use Meta and 43.85% of the respondents use YouTube. Only 30.77% of respondents use LinkedIn and 16.15% of respondents use Pinterest.

2: Considering the Moral Implications

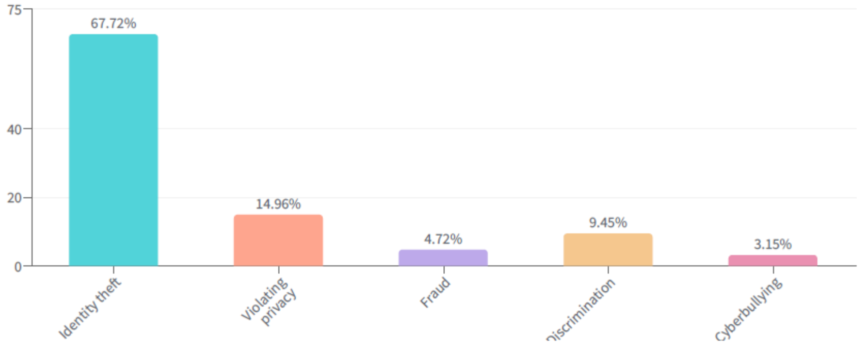

Figure 4: Research method used in researcher data

(Source: Authors' processing)

From the above Figure 2 and Table 2 it can be found that there are 67.72% think that identification of theft can be the key concern while creating social media accounts. 14.96% of respondents think violating privacy 4.72% think fraud as well and 9.45% think discrimination is the major concern. Lastly, there are 3.15% who consider cyberbullying as their major concern.

42.64% of respondents think this is secure to share the information on social media while 57.36% of people think that it is not secure to share the information on social media.

42.97% of respondents are aware of the risk of violating privacy on social media while 33.59% of respondents are not aware of it. The rest of 23.44% of respondents are not aware of this.

In the context of moral considerations, respondents were further asked whether they consider that they have the right to share any private information of another user, the majority of 91.20% have stated that they do not have any considerations to share any private information of other users. On the other hand, the remaining 8.80% of respondents have stated that in the context of moral considerations, they consider having the right to share private information with other users

Moreover, in terms of scaling or rating social media use in terms of ethical agreement with 1 being the lowest and 10 highest, the majority of 41.27% has rated a score 7 which is on the higher terms of the scale. Furthermore, it is also observed that 1.59% of respondents only gave the score of lowest 1, and 2.38% of respondents gave the score of highest response which is a rate of 10.

There are 80.49% who think that identification of theft can break the ethical agreement for the users. 71.54% of respondents think violating privacy 59.35% think fraud as well and 25.20% think discrimination can be the way through which social media users can break the ethical agreement. Lastly, there are 13.82% consider cyberbullying to be a way for social media users to break ethical agreements.

3: A Legal Perspective on Social Media

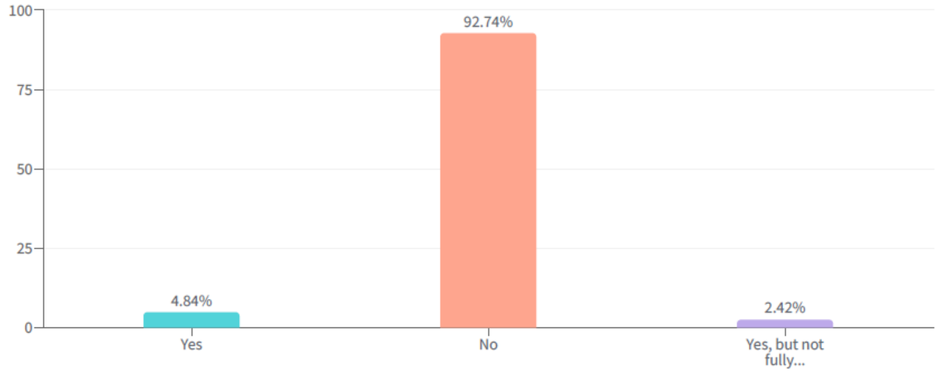

Figure 5: Research method used in researcher data

(Source: Authors' processing)

On the other hand, in the context of social media legal considerations, respondents were asked whether they read social media platforms, "Terms and Conditions" when it comes to privacy and ethical policy. In this accordance, the majority of 92.74% of respondents have stated that they do not read social media terms and conditions in the context of privacy and ethical policy. However, 4.84% of respondents have specified they read social media terms and conditions, whereas only 2.42% have specified that they read but are unable to understand fully.

It can be found that 22.13% of respondents think it is too long to read the whole policy. On the other hand, there are 58.20% of respondents think it's hard to understand, while 4.92% think they don't have enough time to ignore the reading of the policy. Lastly, 6.56% depend on the UAE law for protecting them and lastly, 8.20% of respondents don't believe in the privacy policy. This is the reason they ignore the reading of the privacy policies.

Furthermore, in the context of social media legal considerations, respondents were asked whether they have been subjected to violate privacy while using social media, and most of the respondents 88.62% have not answered. On the other hand, 11.38% responded that yes, they have been subjected to violating privacy while using social media.

4: Online Information Awareness Among Users

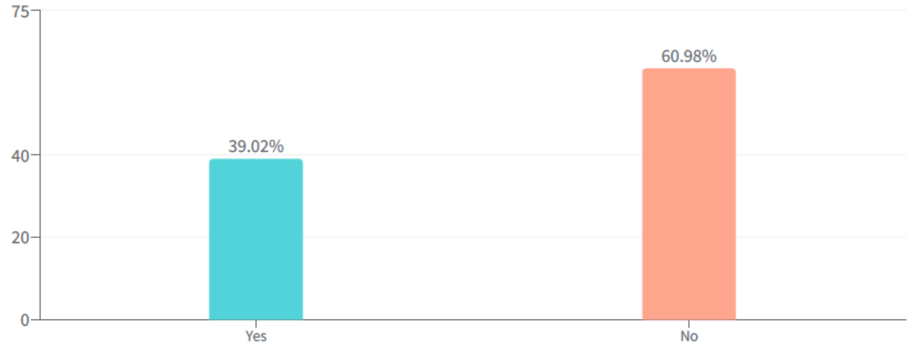

Figure 6: Research method used in researcher data

(Source: Authors' processing)

In terms of giving a response to whether respondents know anyone that were the victim of violating privacy, the majority of 60.98% of respondents have stated that they are not the victim of any violation of privacy. On the other hand, only 39.02% of respondents have stated that they are the victim of violating privacy.

There are only 6.45% and 8.87% of respondents who strongly agree and agree to the fact that whether they share on social media is safe and it's not private for other people to use. On the other hand, 8.06% were neutral regarding this face. There are 45.16% and 31.45% of respondents who have disagreed and strongly disagreed with this fact whether they share on social media is not a safe position.

In terms of user's awareness of their online information, the respondents have been asked for important private information regarding them. The majority of 88.43% have stated that passport information is the most important private information of them. Following that, 87.60% of respondents considered financial information as the most important private information.

Furthermore, 85.95% of respondents have considered hidden addresses as the third most important private information.

It can be identified that there are 50% of respondents think that they won't be able to create a social media account if personal information is not disclosed. 38.52% think that sharing personal information is a normal thing whereas 9.02% need to communicate with others and the rest of 2.46% of respondents are for other reasons.8.26% of respondents think they have full control over the information they share and 85.95% of individuals think they have partial control. On the other hand, 5.79% think they don't have any control.

5: Violating Privacy Rights

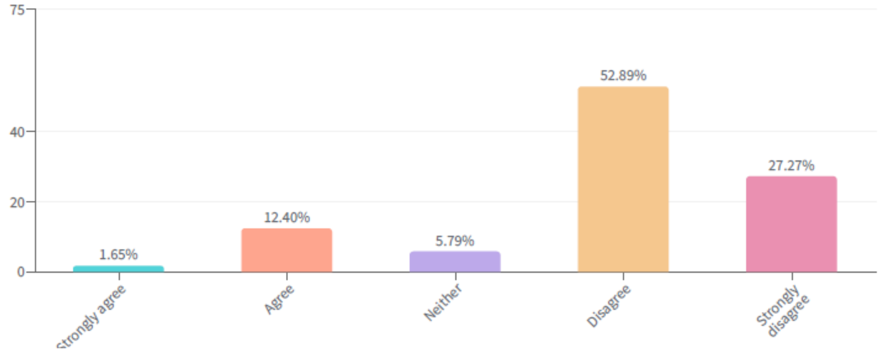

Figure 7: Research method used in researcher data

(Source: Authors' processing)

Only 1.65% and 12.40% of respondents strongly agreed and agreed regarding the fact that social media platforms inform their users about the outcome of disclosing personal information. On the other side, 5.79% were neutral and 52.89% and 27.27% of respondents disagreed and strongly disagreed.

In the context of respondents' considerations of whether personal information is collected and stored safely by social media platforms, it is found that 64.75% of respondents have stated users, social media platforms, and the government all have been ensured. On the other hand, only 6.56% have considered government as the option.

Only 42.15% of respondents have changed their privacy settings to private and 57.85% disagreed with this fact.45.45% of respondents think the government should change the service providers for security whereas 88.43% think they should convey to the users the protection of the information and data. On the other hand, only 31.40% think the government should communicate the laws and the rest of 3.31% of respondents think of other reasons.

Discussion

This study underscores the significance of social media privacy for students, given the digital platforms' ubiquity in their lives. It points out different pressing issues, including privacy setting loopholes, data mining, harassment, location sharing, hacking, and the potential psychological outcomes of excessive use of social media. These concerns are specifically relevant to students who often share a wealth of personal information online. This study also delves into the UAE's legal framework for demonstrating the nation's commitment to safeguarding its residents in the digital realm and protecting digital privacy.

The personal and demographic information section reveals that most students are hyperactive on social media, with most of them using platforms such as Snapchat and Instagram. Many respondents don't read the conditions of these platforms, reflecting a potential shortage of awareness about privacy policies. It demonstrates an important gap in awareness and indicates the need for increased digital education and literacy on social media privacy. However, this study reveals that students are aware of the risks related to identity theft and privacy breaches. This aligns with the growing global concerns regarding personal data misuse and points out the need for comprehensive measures of privacy protection.

In a study of Privacy Awareness of Students and its Impact on Online Learning Participation (Lorenz, 2014), according to their findings, students who engage in the most online socializing are often more conscious of the possible privacy risks associated with this form of communication and want reassurance that they are engaging in safe and secure environments. Furthermore, they have concluded that, when using social networks, students typically don't filter their posts or comments. However, some of them worry if their posts or comments are visible to everyone, their privacy rights may be infringed. Certain environments purport to securely keep data, yet they could sell it to third parties or just have lax privacy controls (Lorenz, 2014).

According to a study conducted on the Internet and Online Information Privacy (Bagchi-Sen, 2022), students who have been exposed to online information privacy through their schools, parents, and the media are more likely to practice online information privacy behaviors, such as avoiding opening emails from senders they are not familiar with, safeguarding personal information, and refraining from downloading files from unidentified individuals or websites (Bagchi-Sen, 2022).

Limitations of the Study

Because this study targets a sample from the University of Sharjah, it is likely to contain many generalizations, as it only examines perceptions of social media privacy among youth in Sharjah and excludes other regions in the UAE. In addition, this study uses a small sample that may not represent the views of all male and female young adults in the UAE. In addition, respondents avoided certain questions and may be biased when answering the questionnaire, which affects the validity of the data. Some respondents were not able to complete the survey due to their busy schedules, resulting in a smaller sample and lower study results.

Conclusion

The findings of this study delivers significant insights in the behaviour and perception of social media users in the study region. These results align significantly with previous research on Emirati, Gulf and Arab college students. Therefore it indicates a significant pattern in considering a concern regarding privacy and ethical implications in the digital landscape.This study points out the significance of social media privacy for students in the UAE. The results specify a high level of use of social media among students, with some concerns regarding identity theft and privacy breaches. It underscores a need for increased awareness campaigns and digital literacy programs to empower all students to safeguard their personal information. UAE's strong legal framework, with penalties for cybercrimes and identity theft, adds an extra layer of student protection. However, as a prospect, it is advisable to conduct a study to gauge students' thoughts on the existing privacy-related legislation in the Emirates. Understanding their viewpoints on these laws could lead to more effective and tailored legal measures to protect students' digital privacy in an ever-evolving online landscape.

References:

1. Abaido, G. M. (2019). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, *25*(1), 407–420. https://doi.org/10.1080/02673843.2019.1669059

2. Abarna, S., Sheeba, J. I., Jayasrilakshmi, S., & Devaneyan, S. P. (2022). *Identification of cyber harassment and intention of target users on social media platforms*. Engineering applications of artificial intelligence. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9364757/

3. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4), 736-758. https://repository.arizona.edu/bitstream/handle/10150/649175/SecretsLikesR1_Submitted.pdf?sequence=1

4. Ahmed, A. (2020). *People accused of cyberbullying face 6 months in jail and a DH150,000 fine in UAE*. UAE – Gulf News. https://gulfnews.com/uae/people-accused-of-cyberbullying-face-6-months-jail-dh150000-fine-in-uae-1.69621180

5. arabianbusiness.com (2022). Revealed: UAE Social Media Laws that can lead to an aed1mn fine. https://www.arabianbusiness.com/culture-society/uae-social-media-laws-to-be-followed-fines-up-to-272mn-if-violated

6. Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29. https://www.researchgate.net/profile/Arwa-A-Al-Shamsi/publication/342887888_Effectiveness_of_Cyber_Security_Awareness_Program_for_young_children_A_Case_Study_in_UAE/links/5f0c14fa299bf1881619832d/Effectiveness-of-Cyber-Security-Awareness-Program-for-young-children-A-Case-Study-in-UAE.pdf

7. Aini, A. P. N., &Alamiyah, S. S. (2022). Privacy management on Instagram users (Qualitative descriptive study of Surabaya's early adults in security management). *Budapest International Research and Critics Institute-Journal,* 5(2). Retrieved October 5, 2022, from https://bircu-journal.com/index.php/birci/article/view/5225

8. Azzi, A., & Dakhane, S. (2022). Social Media and privacy in the UAE: A survey research. *University of Sharjah Journal for Humanities and Social Sciences*, *19*(2),569–604. https://doi.org/10.36394/jhss/19/2/8

9. Bagchi-Sen, S. (2022). *Internet and online information Privacy: An exploratory study of preteens and early teens*. IEEE Transactions on Professional Communication.

https://www.academia.edu/5758734/Internet_and_Online_Information_Privacy__An_Exploratory_Study_of_Preteens_and_Early_Teens

10. Baym, N. K., Cunningham, S., & Craig, D. (2021). *Creator culture. an introduction to global social media entertainment*. New York University Press.

11. Chandra, G. R., Sharma, B. K., &Liaqat, I. A. (2019). UAE's strategy towards the most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(12), 2803-2809. https://www.academia.edu/download/89664937/L30221081219.pdf

12. Child, J. T., & Petronio, S. (n.d.). Communication privacy management theory. SAGE Research Methods. Retrieved September 28, 2022, https://methods.sagepub.com/reference/the-sage-encyclopedia-of-communication-research-methods/i2981.xml

13. Cipolletta, S., Malighetti, C., Cenedese, C., & Spoto, A. (2020). How can adolescents benefit from the use of social networks? The iGeneration on Instagram. International Journal of Environmental Research and Public Health, 17(19), 6952. https://www.mdpi.com/1660-4601/17/19/6952/pdf

14. Dijck, J. V., & Poell, T. (2013). *Understanding Social Media Logic*. https://doi.org/10.12924/mac2013.01010002

15. Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing, privacy, and gendered harassment. The shock and normalization of surveillance cultures. *M&K Medien & Kommunikationswissenschaft*, *68*(3), 273-287.https://scholar.archive.org/work/p7mrhnltkjd75ojme7nkrsp53e/access/wayback/https://www.nomos-elibrary.de/10.5771/1615-634X-2020-3-273.pdf

16. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177. https://link.springer.com/article/10.1007/s40747-021-00409-7

17. Hooper, H. (2017, June 5). An investigation of the role Communication Privacy Management Theory has in the development of social media policies. The Sport Journal. https://thesportjournal.org/article/an-investigation-of-the-role-communication-Privacy -management-theory-has-in-the-development-of-social-media-policies/

18. Latif, M. Z., Hussain, I., Saeed, R., Qureshi, M. A., & Maqsood, U. (2019). Use of smartphones and social media in medical education: trends, advantages, challenges, and barriers. *Acta informatica medica*, *27*(2), 133.-138 https://www.ncbi.nlm.nih.gov/pmc/articles/pmc6688444/

19. Lorenz, B. (2014, July 10). *Privacy awareness of students and its impact on online learning participation–A case study*. IFIP Advances in Information and

Communication Technology. https://www.academia.edu/2876294/Privacy_Awareness_of_Students_and_its_Impact_on_Online_Learning_Participation_a_Case_Study

20. Mehta, A. (2023). *Up to DH1 million fine for violating UAE Social Media Laws: 5 rules you must know*. Khaleej Times. https://www.khaleejtimes.com/legal/uae/up-to-dh1-million-fine-for-violating-uae-social-media-laws-5-rules-you-must-know

21. NA (2023). *Social Media Privacy.* EPIC. https://epic.org/issues/consumer-Privacy /social-media-Privacy /#:~:text=Although%20social%20media%20companies%20typically,users%20%E2%80%9Cconsent%E2%80%9D%20to%20them.

22. Oliveira, T., Araujo, B., & Tam, C. (2020). Why do people share their travel experiences on social media? Tourism Management, 78, 104041. https://run.unl.pt/bitstream/10362/118624/1/Why_people_share_their_travel_experiences_social_media.pdf

23. Petronio, S. (2002). *Boundaries of Privacy: Dialectics of disclosure*. Albany: State University of New York Press

24. Saha, K., Seybolt, J., Mattingly, S. M., Aledavood, T., Konjeti, C., Martinez, G. J., ... & De Choudhury, M. (2021, May). What life events are disclosed on social media, how, when, and by whom?. In Proceedings of the 2021 CHI conference on human factors in computing systems (pp. 1-22). https://dl.acm.org/doi/pdf/10.1145/3411764.3445405

25. Saxena, N. (2021). Upbeat and Downbeat Effects of Social Media in Society: A Critical Review. *Journal of Organisation and Human Behaviour*, *10*(3).https://www.academia.edu/download/89122239/Upbeat_and_Downbeat_Effects_of_Social_Media_in_Society_A_Critical_Review.pdf

26. Swenson-Lepper, T., & Kerby, A. (2019). Cyberbullies, trolls, and stalkers: Students' perceptions of ethical issues in social media. *Journal of Media Ethics*, *34*(2), 102-113.https://www.winona.edu/communicationstudies/media/2019-swenson-lepper-cyberbullies-trolls-and-stalkers.pdf

27. theguardian.com. (2019). *The Cambridge Analytica scandal changed the world – but it didn't change Facebook*. The Guardian. https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

28. UAE (2023). *Cyber Safety and Digital Security: The Official Portal of the UAE government*. Cyber safety and digital security | The Official Portal of the UAE

Government. https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

29. Vomiero, J. (2019) *Facebook logged phone records from Android users with older devices: Reports - national*. Global News. https://globalnews.ca/news/4104435/facebook-scraped-call-text-records-android-devices/

30. 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. https://doi.org/10.1111/j.1083-6101.2011.01559.x

31. Wilmott, C. (2020). *Mobile mapping: Space, cartography and the digital*. Amsterdam University Press.

32. Whitehill, J. M., Trangenstein, P. J., Jenkins, M. C., Jernigan, D. H., &amp; Moreno, M. A. (2020). Exposure to cannabis marketing in social and traditional media and past-year use among adolescents in states with legal retail cannabis. Journal of Adolescent Health, 66(2), 247–254. https://doi.org/10.1016/j.jadohealth.2019.08.024

33. Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485-490.https://par.nsf.gov/servlets/purl/10108920

34. Yang, K. C. C., Pulido, A., & Kang, Y. (2016). Exploring the relationship between Privacy 46 – 62. Kent State University. Retrieved October 5, 2022, from https://www-s3-live.kent.edu/s3fs-root/s3fs-public/file/K-YANG-A-PULIDO-Y-KANG.pdf.

Appendices

Part 1: Demographic and Personal Information

1. **Gender?**
a. Male
b. Female
2. **Age?**
a. **18-20**
b. **20-22**
c. **22-24**

3. **Education?**
c. Undergraduate
d. Post-graduate

4. **Do you own and operate at least one social media account?**
e. Yes
f. No

5. **How long have you been using social media platforms?**
g. **6 – 12 months**
h. **1 – 2 years**
i. **3 – 4 years**
j. **5 – 6 years**
k. More than 6 years

6. **Which social media platform are you most active on? (Multiple answers)**
l. Instagram
m. Twitter
n. Facebook
o. Snapchat
p. YouTube
q. LinkedIn
r. Pinterest

7. **How much time on average do you spend on social media every day?**
s. Half an hour
t.**1 – 2 hours**
u. **3 – 5 hours**

v. **6 – 8 hours**
a. More than 12 hours

Part 2: Considering the Moral Implications

8. **What was your main concern when you created your social media account?**
a. Identity theft
b. Fraud
c. Discrimination
d. Cyber bullying

9. **Are you aware of how secure the information you share on social media is?**
a. Yes
b. No

10. **Are you aware of the risks of violating another user's privacy?**
a. Yes
b. No
c. Not concerned

11. **Do you consider that you have the right to share any private information of another user?**
a. Yes
b. No

12. **On scale 1 – 10, rate your social media use in terms of ethical agreement with 1 being the lowest and 10 the highest.**

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

13. **In the UAE, what do you think are the ways that social media users can break the ethical agreement. (Multiple answers)**
a. Identity theft
b. Fraud
c. Discrimination
d. Cyber bullying

Part 3: Legal Perspective on Social Media

14. **Do you read social media platforms "Terms and conditions" when it comes to privacy and ethical policy?**
   a. Yes
   b. No
   c. Yes, but not fully understand

15. **If your answer to the previous question is no, what are the reasons for you to ignore the reading the policy?**
   a. Too long
   b. Hard to understand
   c. Do not have the time
   d. Perceive that the UAE law will protect you
   e. Do not believe in the privacy policy

16. **Have you been subject to harassment, or bullying while using social media**
   a. Yes
   b. No

17. **If your answer to the previous question is yes, how would you rate the following statement: "The experience was very shocking, humiliating and painful".**
   a. Strongly agree
   b. Agree
   c. Neither
   d. Disagree
   e. Strongly disagree

18. **If your answer to the previous question is no, do you know anyone that were victims of cyber bullying?**
   a. Yes
   b. No

19. **How would you rate the following statement: "I believe that the information I share through social media is safe and private for other users to use"**
   a. Strongly agree
   b. Agree
   c. Neither
   d. Disagree
   e. Strongly disagree

Part 4: Online Information Awareness Among Users

20. **What of the below would you concerned 3 most important information?**
    a. Name
    b. Nationality
    c. Home address
    d. Personal Picture
    e. Family members
    f. Personal phone number
    g. Financial information
    h. Passport information
    i. Medical information
    j. Work history
    k. Friends
    l. Others

21. **What is the reason for you to disclose personal information on social media platforms?**
    a. You are not able to create an account if personal information is not disclosed
    b. Disclosing personal information has become a normal thing in our daily lifestyle
    c. To connect with others
    d. Others

22. **How much control do you believe you have over the information you disclosed on social media platforms (ability of change, delete, or correct)?**
    a. Full control
    b. Partial control
    c. None

23. **How would you rate the following statement: “Social Media platforms appropriately inform their users about the consequences of disclosing personal information?**
    a. Strongly agree
    b. Agree
    c. Neither
    d. Disagree
    e. Strongly disagree

24. **Who do you think should ensure that personal information is collected and stored safely by social media platforms?**

a. Users
b. Social Media platforms
c. The Government
d. All the above

25. **Did you change your privacy setting to private once you finished setting up your social media account?**

a. Yes
b. No

Part 5: Violating Privacy Rights

26. **What do you think the role of the government is in protecting the user's privacy should be (Multiple Answer)?**

a. Change the service providers for security
b. Convey the user's on how to protect their data and information
c. Communicate the laws
d. Others

27. **What do you think the role of the user is in protecting their privacy should be (Multiple Answers)?**

a. Maintain their privacy by not sharing private content on social media
b. Be aware of the privacy policy and rules given by the government
c. Report any suspicious users
d. Others