The Impact of Privacy Laws on Social Media in the United Arab Emirates

تأثير قوانين الخصوصية على وسائل التواصل الاجتماعي في دولة الإمارات العربية المتحدة

by

ABDELRAHMAN AHMED ALMULLA ALHAMMADI

Dissertation submitted in fulfilment

of the requirements for the degree of

MSc IT MANAGEMENT

at

The British University in Dubai

November 2018

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author’s express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

Acknowledgement

First, I would like to thank Allah Almighty for giving me the strength, knowledge, ability and opportunity to undertake this challenge and follow through to its completion. It is with the grace of Allah that this achievement was possible.

Second, I would like to thank my research supervisor Dr. Cornelius Ncube for his continuous support during my research. Dr. Cornelius Ncube who have been supportive of my career goals and who worked actively to provide me with the protected academic time to pursue those goals.

Most importantly, I wish to thank my loving and supportive wife, Esra, and my daughter Amina, who provides me unending inspiration.

Finally, I would like to thank The British University in Dubai for providing me with this opportunity and giving me the chance to study in this world-class environment for research and development. It has been a pleasure meeting such great people from all over the world, from the university staff who provided mentorship and guidance, to my colleagues who became some of my closest friends.

Sincerely,

Abdul Rahman

English Abstract

The purpose of this research is to perform a study on the impact of privacy laws on social media. This discussion demonstrates that there is no single definition of privacy that is applicable to all features of social media and that it is often necessary to combine perspectives to achieve a holistic framework that can guide research on issues of both information disclosure and privacy.

This research is based on an Epistemology research methodology; as this methodology is focused on the facts that determine the acceptable knowledge about the concerned field of research as well as it also question the information known to be true on the basis of rigorously tested and treated facts. Furthermore, results examined that social networking privacy laws are followed by the UAE social networking websites but not by all.

In the conclusion of this research, the measures to determine the privacy law's impact on personal information policies, control and notification to measure the acceptance of social networking websites by users and risk awareness in determining social networking acceptance by users are discussed. And the results concluded that that privacy laws and concerns for control and notification affected the user's acceptable behavior and the UAE authorities must follow such measures that guarantee the protection of sensitive information and other personal details.

Arabic Abstract

الغرض من هذا البحث هو إجراء دراسة حول تأثير قوانين الخصوصية على وسائل التواصل الاجتماعي. توضح هذه المناقشة أنه لا يوجد تعريف واحد للخصوصية ينطبق على جميع ميزات الوسائط الاجتماعية وأنه من الضروري في كثير من الأحيان الجمع بين وجهات النظر لتحقيق إطار عمل شامل يمكن أن يوجه البحث في قضايا الإفصاح عن المعلومات والخصوصية.

يعتمد هذا البحث على منهجية البحث المعرفية. حيث أن هذه المنهجية تركز على الحقائق التي تحدد المعرفة المقبولة عن مجال البحث المعني، كما أنها تشكك في المعلومات المعروفة على أنها صحيحة على أساس الحقائق التي تم اختبارها ومعالجتها بدقة. علاوةً على ذلك، تفحَّصت النتائج أن قوانين الخصوصية للشبكات الاجتماعية .تتبعها مواقع الشبكات الاجتماعية في الإمارات العربية المتحدة ولكن ليس من قبل الجميع.

في ختام هذا البحث، تمت مناقشة التدابير لتحديد تأثير قانون الخصوصية على سياسات المعلومات الشخصية والتحكم والإشعار لقياس قبول مواقع الشبكات الاجتماعية من قبل المستخدمين والوعي بالمخاطر في تحديد قبول الشبكات الاجتماعية من قبل المستخدمين. وخلصت النتائج إلى أن قوانين الخصوصية والمخاوف المتعلقة بالرقابة والإخطار تؤثر على سلوك المستخدم المقبول ويجب على السلطات الإماراتية اتباع الإجراءات التي تضمن حماية .المعلومات الحساسة والتفاصيل الشخصية الأخرى.

Table of Contents

List of figures

List of tables

Acronyms and Abbreviations

ANOVA	-	Analysis of variance
BBS	-	Bulletin board systems
EEA	-	European Economic Area
ENISA	-	European Union Agency for Network and Information Security
EU	-	European Union
GDPR	-	General Data Protection Regulation
IP	-	Internet Protocol
IRC	-	Internet Relay Chat
MRQs	-	Main Research Questions
OSN	-	Online Social Network
SMPC	-	Social media privacy concerns
SPSS	-	Statistical Package for the Social Sciences
UAE	-	United Arab Emirates
US	-	United States

Chapter 1. Introduction

1.1 Background

Human Race is destined to evolve and advance in numerous facets of life. The aspiration of Mankind to examine and explore a better life or a better world has caused them to evolve from a caveman to the current attributed social being. The inclination of humans towards living in a society has created various tools and mediums of communication. This later improved to the modern civilizational languages and technology. Technology itself has been ever evolving, from an abacus to mainframes, Mainframes to Personal Computers and laptops, Cassettes, Floppies, Hard Disk Drives, USB to Cloud computing. A Transmitter or a pager once has now evolved to be the latest smart phone.

All of this advancement in technology has united the physical human world with computerized horizons, enhancing the functionality of time, cost and work to an ultimate user experience.

Information Technology has altered the course of human communication. An effective and convenient communication is made possible through the means of mobile phones and handheld devices, be it for personal or professional usage.

Earlier, chat rooms were created to connect and socialize on internet, like Bulletin board systems (BBS), Internet Relay Chat (IRC), Instant messengers and blog sites etc.; however, they were not as popular and as user friendly as the modern day social networking platforms.

Modern day socializing which is also known as social networking is media and content sharing through blogs, websites and applications. These interconnect with each other to gather a massive populace of content and users for a better and enlarged connectivity through various privacy rules & regulations. Figure 1 illustrates the graphical representation as such:

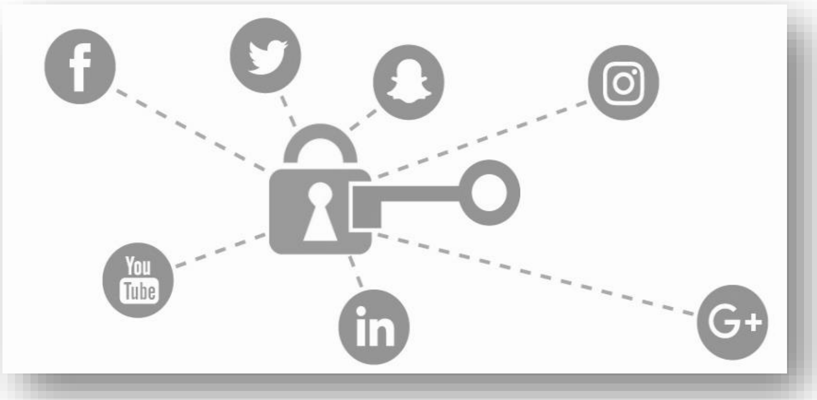

Figure 1 Social Media and Privacy

The accumulative usage of technology and social networking for text messages, pictures and videos sharing, newsfeeds, online education, e-commerce, online events and conferences have altogether developed the modern internet world.

Enormous benefits of social media and its massive usage has raised the significance of security and privacy. Privacy is the vital right and concern of any individual or a group of people, users may limit the sharing and usage of their information.

Information privacy has been described as confidentiality, secrecy and anonymity (Margulis, 2003). Westin (1967) referred to information privacy as the user ability to control his or her personal information. Information privacy in the field of information systems has predominantly focused on measurement of privacy concern constructs (e.g. Malhotra et al., 2004; Slyke et al., 2006; Dinev and Hart, 2005, 2006; Youn, 2009; Xu et al., 2008)

1.2 Major Privacy Concerns in Social Media

The Modern day social media is acclaimed with the reality of mankind and thus difficult to separate among the two, so is the privacy of its user. Enhanced and increased measures of network security call upon the definite importance of user privacy.

1.2.1 Account hacking and impersonation

Social Media has become a paradise for hackers and spammers, an easy and effective way to stalk several accounts or impersonating them, spreading different malwares, viruses and scams. Social Media is actually much more exposed and efficient for cyber criminals than the old-style email spams. A user with less awareness of cyber security may fall to these traps much easily, trusting the content from unknown or fake sources and as a result getting their devices infected and their data hacked through social media.

1.2.2 Location

A Prime number of users access their social media through handheld devices, such as smartphones and tablets. Social media applications offer several benefits of location-based services to be enjoyed through smart devices, which might be a potential privacy threat for its user. In fact, these applications continue to collect user data and location which is eventually used by social media sites and applications for their very purposes.

The lack of regulatory bodies or the governance of privacy laws has allowed a significant liberty to social media service providers in administration of user data and information. Hackers and Prowlers take benefit of user data or location in execution of online thefts and frauds.

1.2.3 The privacy tree

Default or inherited privacy settings such as public or sharing with friends of friends may mark any individual vulnerable to the breach of privacy. The privacy is commonly a complex or obscure matter for everyday users. The lack of understanding in setting up privacy may result a post or information to be shared in numerous circles outside the specific circle of user, which however was intended for a specific audience in a specific group. Users may trust their privacy to be dissected, yet the privacy tree have many branches.

1.3 Problem Statement

It is very common now a day to have breach of privacy in social media and this breach could cause a lot of problem in one’s life if any personal information is exploited or misused. The new interests of service providers, making money through commercializing social media may have these companies expending user information into monetary benefits. The other major problem is not limited to the usage of personal information as a commercial tool but its exposure to other users or service providers.

Personal information such as age, gender, locality and the interests of a user are among the basic information which is provided to social media websites and is often used for their benefit. For example, Facebook, which is a free social networking service, trades this user data for running ads or trading with other companies for business purposes.

Data Privacy is a joint responsibility of the user and the social media service providers. A user must be aware of the influence of their shared content on social media and should take great caution when providing personal information to social media websites.

The search engine ASK.COM has allowed their users to delete personal information or data opting “using the eraser”. This option enables the user to search their personal data and delete it if required. The European Union Agency for Network and Information Security (ENISA) has emphasized a great deal on digital privacy and other concerning issues arising out of it. According to Security Issues and Recommendations for Online Social Networks 2007, ‘users have the right to erase any comment or any information on the network and close their account on any social media website and delete their personal files except on Facebook’. A Facebook user is able to activate their account any time if the user has only deactivated the account. The pact for the protection of user’s information is trivial in ‘Terms of Agreement’ between social networking websites and their users.

To come across the above challenges, an analysis is proposed in our study to examine the privacy protection law on social media and to sentry the posting of information of a minor on social media, considering the law may vary from country to country.

1.4 Study Scope

The scope of this study is to analyze the impact of privacy laws and regulations in the UAE, discussing:

- Privacy concerns with personal information policies
- Risk awareness
- Control and Notification
- Deleting information.

1.5 Study Aim

Privacy laws and regulations of social media recounts a person's right to privacy and to protect one's privacy from any potential threat. Privacy laws may differ based on regional or industrial location. A country, state or region may constitute its own law for personal privacy or data protection of individuals.

Workplace ethics and employer's manifesto of employees' code of conduct may administer the activities of their employees on social media. Some Countries and Regional laws are also instigated on the fair use of social media.

This study aims to understand the impact of privacy laws in social media in the UAE.

1.6 Study Objectives

The above stated aim elevate the following essential study objectives:

- Analyzing the nature and impact of privacy concern on social media in the UAE.

- Identifying factors impacting privacy concern on social media in the UAE
- Providing recommendations to users to increase privacy level on social media in the UAE.

1.7 Significance of the Study

1.7.1 Theoretical Aspect

This study will contribute in significance to comprehend the influence of privacy laws and regulations governed in a country. The study will reveal several aspects of process implementation.

1.7.2 Applied Aspect

The research study would deliver details on the subject of policy making in privacy laws and regulations in the UAE. Additionally, this study could assist in the implementation of privacy laws and regulations. This could eventually provide aid to the legislative authority in appliance of a contemporary policy. The research study can be a start point for the upcoming academics on the recent information and status of the subject.

1.8 Research Conceptual Framework and Hypotheses

Online socializing or networking websites and the protection of user information are to be balanced naturally. Social media platforms are intended to share their users' life in public and to its quite conflict protecting the privacy of their users, altogether. A number of measures and approaches are adopted to assure the online privacy of social media users and several laws have been passed globally for online security.

1.8.1 Research Null Hypothesis

It is hypothesized, the impact of privacy laws in social media websites in the UAE.

1.9 General Data Protection Regulation (GDPR)

1.9.1 Introduction

The General Data Protection Regulation (GDPR) is the new regulation that will substitute the previous version which was introduced in 1995 when the internet was in its beginning phase. Whereas, in modern era the privacy and security concerns have increased to a great extend due to the higher number of users on social media and companies such as Google and Facebook amassing huge amount of personal information of their users.

GDPR was introduced on 14th April 2016 and formally accepted on 25th May 2018 by European Union on data and privacy protection for all individuals within the European Union (EU) and the European Economic Area (EEA). This regulation is for individual users' data only and does not apply on businesses.

1.9.2 Main GDPR Concept

Personal privacy

- The user to have the right and ability to access all personalized data when and wherever the user wants, while having the ability to delete and download the data.

Control and notification

- The user to be notified, if any intrusion or interruption occurs in the last 72 hours.

- The consent of user to be asked about the organization's use of user's personal data.
- The user to be kept informed regarding any work or activity being done on user data

Transparent policies

- Clear procedures as how the data is calculated and when it is processed.

Clear deleting policies

- The right to forgotten, user can ask to wipe off the personal data and stop the processing of this data in article 17; if the data is no longer part of the original purpose the user may erase it.

Retention policies

- GDPR advantage to user data
  i. Data Governance, Stringent control on user data. Where, for what and how user data is collected and used.
  ii. Compel the social media company to justify their use of users' data.
  iii. The user to give detailed consent to the company as for what user's data can and cannot be used.
  iv. Personal data may contain name, phone number, user account detail, social media posts, email address, IP address, health data and political opinion of users.

1.9.3 Penalties for non-compliance

Non Compliance to any or all features of GDPR may result in the company to be fined for up to 20 Million dollars or 4% of their annual international income from the web. It may also include; unavailability of user's consent agreement, failure to notify the user in case of breach of data or if the data is leaked or hacked.

1.9.4 Clear Acceptance unambiguous data collection

User protection is amplified in GDPR as it clearly describes the procedures of data collection. The user must give a clear consent and acceptance for data gathering. The consent agreement must be easy to read and understand. The purpose of data gathering should be clear, ethical, without any confusion or swindle of words or in the text. Furthermore, the user can get the copy of his data without any fee or charges.

A. Limitation of data collect

GDPR requires the companies to limit the amount of data gathering and processing. It compels them to reduce the use of personal information to maximum extent.

B. Parental consent -B

The parents of a child, who is under 16 years of age, have the right to keep a check on their child through expressing consent and the same rule is anticipated for the European Union member until the child is 13 years of age.

1.9.5 GDPR and global reach

GDPR has a global reach; it covers a huge part of the globe. GDPR not only covers the European Union but also any company that is located outside the Europe but is providing any service in Europe or administering the interests of people located in Europe. A company may be operating outside the European Union but still might be regularized by GDPR, if any of their client is located in Europe or any services provided therein.

1.9.6 Facebook and GDPR

Facebook has verbally endorsed the "General Data Protection Regulations". The company has not fully incorporated the new EU standards. On their website, Facebook claims to comply with the current EU's data protection law which came into effect on 25 May 2018. Their GDPR preparations were led by headquarters in Dublin, Ireland.

However, according to Kanner, 'it is just a matter of time, since most of the companies would be moving towards securing their data, not only for the customers but also to protect the data they share with other companies'.

1.9.7 UAE Industry and global reach

Amit Roy, Executive Vice-President and Regional Head for EMEA at Cyber security firm Paladion, mentioned that many companies in UAE are implementing GDPR, some companies started the implementation earlier however they did not complete the implementation entirely. As per him 30% to 40% companies have managed to implement. Moreover, there is a huge volume of trading trend between EU and UAE. The European

Union is one of the key trading partners of the UAE and the both sides have trades up to US $ 65.8 billion in 2016 only. UAE is one of the top ten destinations for EU exports. Almost 41,000 European companies and 121,000 citizens of European Union are inhabited in UAE

1.9.8 The international financial center in Abu Dhabi and Applying GDPR

The protection of data security is safeguarded in the office of Registration Authority in the international financial center in Abu Dhabi, with the assignment to spread over GDPR in the international financial center. The official approach is to create a leading global financial center which provides secure services to its clientele as per internationally recognized standards. Its primary objective is to ensure a reliable atmosphere for business and individual customers. Applying GDPR includes gathering, analyzing, classifying, protecting and assembling accessible data to ensure overall privacy for individual and corporate clients.

Chapter 2. Literature Review

Millar (2006) carried out a research towards a legal obligation to adopt reasonable information security procedures exists in a variety of laws around the world, such as the EU Data Directive (Directive 95/46), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and sectoral and state privacy laws in the U.S. The latter include security breach notification laws, and laws establishing a general duty of security. This paper compares and contrasts the privacy and information security landscape inside and outside the U.S. and offers suggestions for corporate “best practices” in data security designed to enhance consumer trust and minimize liability.

Vladlena B, George S and Hemamaali T (2015) conducted a research on Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? They investigated the link between information disclosure, control over personal information, user awareness and security notices in the social context, all of which are shown to be different from existing studies in e-commerce environments. Based on their analysis they showed that in social networking contexts, control over personal information is negatively and statistically associated with information disclosure. However, both user awareness and security notices have a positive statistical effect on information disclosure.

Elizabeth A, Anne L.R, Dhruv Grewal and Martin W (2016) researched on the personalization-privacy paradox: implications for new media. They investigated personalized communications through digital media, which include display, search, social and mobile communications. Personalization can both enhance and diminish consumer engagement with the firm: it may heighten privacy concerns because consumers worry about how their data are collected and used, and it can also benefit them in meaningful ways. Thus, firms must use the information that they collect in a strategic manner to balance this personalization-privacy paradox. This paper finds that the benefits of personalization may vary as a function of the medium through which the communication is conveyed. It suggests directions for research in each of these media and strategies firms can implement to mitigate privacy concerns. This investigation of emerging themes related to search, display, social and mobile communications provides a more comprehensive overview of current research, as well as a foundation for further research into personalization.

Christian F (2011) conducted a research to challenge the liberal notion of privacy and explore foundations of an alternative privacy conception. Given the criticisms advanced in this paper, the need for an alternative, socialist privacy concept is ascertained, and it is argued that privacy rights should be differentiated according to the position individuals occupy in the power structure, so that surveillance makes transparent wealth and income gaps and company's profits and privacy protects workers and consumers from capitalist domination.

The paper contributes to the establishment of a concept of privacy that is grounded in critical political economy. Owing to the liberal bias of the privacy concept, the theorization of privacy has thus far been largely ignored in critical political economy. The paper contributes to illuminating this blind spot.

Valerie S. and Priscilla R (2014) carried out a study to develop a conceptual framework to contextualize young people's lived experiences of privacy and invasion online. Social negotiations in the construction of privacy boundaries are theorized to be dependent on individual preferences, abilities and context-dependent social meanings.

Empirical findings of three related Ottawa-based studies dealing with young people's online privacy are used to examine the benefits of online publicity, what online privacy means to young people and the social importance of privacy. Earlier philosophical discussions of privacy and identity, as well as current scholarship, are drawn on to suggest that privacy is an inherently social practice that enables social actors to navigate the boundary between self/other and between being closed/open to social interaction.

Four understandings of privacy's value are developed in concordance with recent privacy literature and our own empirical data: privacy as contextual, relational, performative and dialectical.

A more holistic approach is necessary to understand young people's privacy negotiations. Adopting such an approach can help re-establish an ability to address the ways in which privacy boundaries are negotiated and to challenge surveillance schemes and their social consequences.

Findings imply that privacy policy should focus on creating conditions that support negotiations that are transparent and equitable. Additionally, policy-makers must begin to critically evaluate the ways in which surveillance interferes with the developmental need of young people to build relationships of trust with each other and also with adults.

Wilton (2017) conducted a research aims to provide a non-academic perspective on the research reports of the JICES "Post-Snowden" special edition, from the viewpoint of a privacy advocate with an IT background.

This paper was written after reviewing the country reports for Japan, New Zealand, PRC and Taiwan, Spain and Sweden, as well as the Introduction paper. The author has also drawn on online sources such as news articles to substantiate his analysis of attitudes to technical privacy protection post-Snowden.

Post-Snowden, the general perception of threats to online privacy has shifted from a predominant focus on commercial threats to a recognition that government activities, in the sphere of intelligence and national security, also give rise to significant privacy risk. Snowden's disclosures have challenged many of our assumptions about effective oversight of interception capabilities. Citizens' expectations in this regard depend partly on national experience of the relationship between citizen and government and can evolve rapidly. The tension between legitimate law enforcement access and personal privacy remains challenging to resolve.

As a "viewpoint" paper, this submission draws heavily on the author's experience as a privacy and technology subject-matter expert. Although it therefore contains a higher proportion of opinion than the academic papers in this issue, his hope is that it will stimulate debate and further research.

(Kosta, Kalloniatis, Mitrou & Gritzalis, 2010) conducted a study to examine how the introduction of new communication channels facilitates interactive information sharing and collaboration between various actors over social networking services and how social networking fits in the existing European legal framework on data protection. The paper also aims to discuss some specific data protection issues, focusing on the role of the relevant actors, using the example of photo tagging.

Privacy in social networks is one of the main concerns for providers and users. This paper examines the role of the main actors in social networking, i.e. the providers and the users, scrutinized under the light of the European data protection legislation. Specifically, how social networking service providers deal with users' privacy and how users handle their personal information, if this manipulation is complied with the respective legislation and how “tagging”, one of the most familiar services provided by the social networking providers, may cause privacy risks.

Social networking is one of the most remarkable cultural phenomena that has blossomed in the Web 2.0 era. They enable the connection of users and they facilitate the exchange of information among them. However, the users reveal vast amounts of personal information over social networking services, without realizing the privacy and security risks arising from their actions. The European data protection legislation could be used as a means for protecting the users against the unlawful processing of their personal information, although a number of problems arise regarding its applicability.

The paper discussed some privacy concerns involved in social networks and examines how social networking service providers and users deal with personal information with regard to the European data protection legislation.

(Kosta, Kalloniatis, Mitrou & Gritzalis, 2010) conducted a study to build a research model that examines social media privacy concerns (SMPC) in relation to users' trusting beliefs and risk beliefs.

An instrument with eight constructs (SMPC: collection, SMPC: secondary usage, SMPC: errors, SMPC: improper access, SMPC: control, SMPC: awareness, trusting beliefs and risk beliefs) was developed and administered to subjects from a mid-sized university in the USA. Collected data were analyzed using partial least square structural equation modeling.

The results showed that three of the six SMPC (i.e. secondary usage, improper access and awareness) were negatively and significantly associated with users' trusting beliefs. In addition, three of the six SMPC (i.e. collection, errors and improper access) were positively and significantly associated with users' risk beliefs.

Practical implications were aimed at the social media sites to design simple and straightforward privacy policy statements that are easy to understand; to safeguard users' online privacy behaviors; and to develop mechanisms to protect personal information.

This study enhances the literature by contributing to a generalized knowledge of SMPC of users as they relate to their trusting beliefs and risk beliefs.

(Pierson & Heyman, 2011) studied how the advent of Web 2.0 or so-called social media have enabled a new kind of communication, called mass self-communication. These tools and the new form of communication are believed to empower users in everyday life. The authors of this paper observe a paradox: if this positive potential is possible, the negative downside is also possible. There is often a denial of this downside and it is especially visible in social media at the level of privacy and dataveillance. The purpose of this paper is to illustrate this point through an analysis of cookies.

The paper illustrates how mass self-communication in social media enables a new form of vulnerability for privacy. This is best shown by redefining privacy as flows of Personal Identifiable Information (PII) that are regulated by informational norms of Nissenbaum's concept of contextual integrity. Instead of analyzing these contexts on a general level, the paper operationalizes them on the user level to illustrate the lack of user awareness regarding cookies. The results of the research were gathered through desk research and expert interviews.

The positive aspects of cookies, unobtrusiveness and ease of use, are also the main challenges for user privacy. This technology can be disempowering because users are often hardly aware of its existence. In that way cookies can obfuscate the perceived context of personal data exposure.

(Kayes & Iamnitchi, 2017) discussed the current techniques and attack strategies for future directions of research by studying the social networking becomes increasingly important due to the recent surge in online interaction. Social network analysis can be used to study the functioning of computer networks, information flow patterns in communities, and emergent behavior of physical and biological systems. In this paper, the mathematical formulation and computational models for security and privacy of social network data are discussed. Several possible ways for an attacker to attack are presented so that the mathematical formulation can take them into account. The metrics for measuring the amount of security and privacy in an online social network (OSN) are discussed so that we have an idea of how good a model is.

Chapter 3. Research Methodology

The selection of research philosophies plays a vital role in further planning and carrying out of the research. Below figure 2 depicts the layers of this research as how they have been done with.

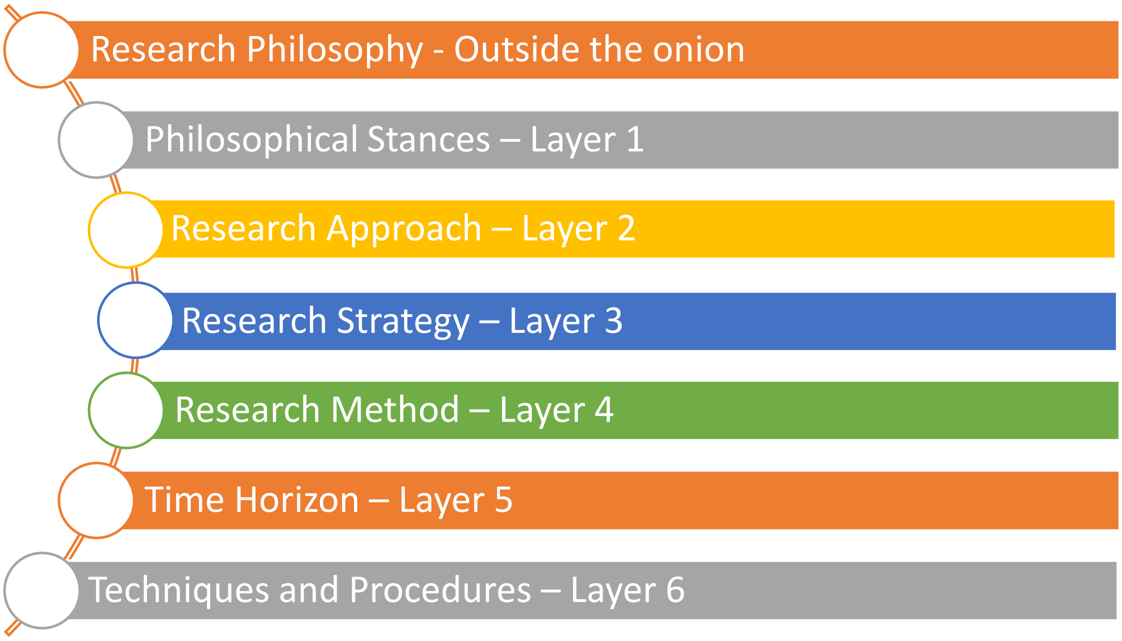
Research Philosophy - Outside the onion
Philosophical Stances – Layer 1
Research Approach – Layer 2
Research Strategy – Layer 3
Research Method – Layer 4
Time Horizon – Layer 5
Techniques and Procedures – Layer 6

Figure 2 Layers of Research Methodology

3.1 Research Philosophy – Outside the onion

The selection of research philosophies plays a vital role in further planning and carrying out of the research. There are three types of research philosophies and among them only one can be applied at a time based on the requirements and specifications of the research; these philosophies are Ontology, Epistemology and Axiology. Ontology is basically the study of the nature of reality while the Axiology is the philosophy which provide the chance to understand the impact of values and opinions of the research over the collection and analysis of the research related data (Biesta, 2015). However, the Epistemology is focused on the facts that determine the acceptable knowledge about the concerned field of research as well as it also question the information known to be true on the basis of rigorously tested and treated facts.

Since the focus of this paper is to study the impact of the privacy laws on social networking sites in the UAE so this seems to incur facts and information that is tested and proven to be true. In this regard, the Epistemology will be applied on this study, so the research can consider the information and facts that can be proved without any uncertainty. The epistemology can be applied to this study as it is one of the most commonly used philosophy for the field of scientific research (Smarandache, 2016). However, the selection of this philosophy will proceed to the options of philosophical positions associated with it; and so, there are three options for the philosophical stances including positivism, critical realism and interpretivism.

3.2 Philosophical Stances – Layer 1

The first layer of research onion consists of philosophical stances which are associated with the research philosophies. While there are multiple options available under the head of philosophical stances, but it completely depends on the research philosophy that which options are available for the particular study (Joslin & Müller, 2016). The philosophical stances can be Objectivism, Constructivism, Positivism, Realism, Interpretivism and Pragmatism. Whereas since this study is based on Epistemology so the only options of philosophical stances available for this study Are Positivism, Critical Realism and Interpretivism. In Positivism, hypotheses are generated along with Main Research Questions (MRQs) which then can be tested allowing the explanations that can be measured against the accepted knowledge. The information created from this research can be replicated by others in order to generate the similar results. The results of Positivism are focused to be quantifiable which lend to statistical analysis.

On the other hand, Critical Realism is almost similar to the positivism in terms of processes while it consider that research and social reality are independent to each other, therefore results cannot be biased (Howes, 2017). Whereas it differs from positivism when it claims that scientific methods are not reliable and so one should keep researching continually while incorporating new research methods. In addition to this, the Interpretivism is the approach which emphasize the meaningful nature of participation of people in cultural and social life. It basically assesses the perceptions of people on the basis of their own actions and the actions of others.

As the study is concerned about studying the impacts of privacy laws in social networking web sites so in this regard Interpretivism is considered to be the best suited philosophical stance for the research. The interpretivism support the analysis of perspective of people confer upon their own actions as well as upon the actions of others. While this stance contains a view that change and cultural existence can only be understood appropriately when the perceptions of different people will be studied along with the study of their ideas, and their priorities.

3.3 Research Approach – Layer 2

The second layer of research onion demands the decision regarding the appropriate research approach. While this decision is based on the research aim, limitations, philosophical stance as well as personal opinion about the appropriate approach (Singh, 2015). There are only two options in this level and only one can be applied at a time; the options include Deductive approach and Inductive approach.

In deductive approach the study is initiated by a question or a statement leading towards the answer while aim of the study would be concluded by a positive or negative response in this approach. The procedure followed under this research approach will move from the generalized theory to research questions and data collection proceeding towards findings which either reject or accept the research question. While on the other hand the inductive approach is focused on creating theory and work process of this approach will be opposite to deductive. Inductive approach does not rely on existing theory and so proceed from research question to observation and description which further lead to analysis and final theory (Quinlan et al., 2018).

As the study focused here, consists of research aim which need to be assessed for the acceptance or rejection so the Deductive approach will suites the best for this paper. The procedure followed for the conduction of the research will be from generalized to specific starting from the theory and ends on confirmation of research question’s acceptability or rejection.

3.4 Research Strategy – Layer 3

The third layer of the research onion is focused on the research strategies which are the styles used for the collection and analysis of the data. There are multiple strategies which can be used for the research as per the requirement and the decision is made on the basis of philosophies and philosophical stances. Here one or more than one choices can be made for a single study and a combination of different strategies can be used to collect and analyze the data. The options may include Experiments, Survey, Case Study, Action Research, Grounded Theory, Ethnography and Archival Research. All of these strategies have their own specific features and specifications which may vary on the basis of their use (Sekaran & Bougie, 2016).

This paper has chosen Epistemology and Interpretivism in the options for philosophies and philosophical stances respectively and focused on studying the impacts of privacy laws in the UAE regarding the social networking websites. In this regard, Survey strategy is applied over this study which is associated with the deductive approach providing the economical way for the collection of large quantity of data. This will further aid in addressing the what, who, where, how and when of the concerned topic of social media privacy by generating statistical data.

3.5 Research Method – Layer 4

The fourth layer is about the choice of research method determining the type of research to be used. Here the question is asked for the selection of Qualitative Research Method or Quantitative Research Method while confirming the way of using these methods. It is when the decision is required to be made that whether to use only one method or use a combination of two. The quantitative method is based on quantities and measurements while focused on numbers (Soy, 2015). While on the other hand the qualitative research method is focused on the opinions, description and personal perspectives and concerns. However, there are three ways in which these methods can be used; mono method, mixed method and multi method.

Mono method is when any one of the methods is being used among qualitative and quantitative. Mixed method is when mixture of both the methods is being used for the conduction of the research. Multi method is when both methods are used but one of them is particularly focused (Sekaran & Bougie, 2016). Here for this study Mono Method is used as only Quantitative Research Method is being incorporated as the assessment is based on quantities.

3.6 Time Horizon – Layer 5

The fifth layer of the research onion determine the time horizon which determine the duration in which the research is planned to be conducted. There are two main options and only one can be applied at a time in one paper; the options are cross sectional or longitudinal. The cross sectional is short termed whereas the longitudinal is a long termed research. Cross sectional is particularly used for the measuring any concerned aspect in a single point of time and it can be used for both types of researches, qualitative and quantitative (Vamsi et al., 2014). Contrary to that longitudinal can also be used in both types of researches but it is for the conduction of a research over a longer time duration such as research conducted for 5 years or more. This study is only considering the current impacts of the privacy laws in the UAE so cross sectional time horizon is being selected for this particular paper.

3.7 Techniques and Procedures – Layer 6

The sixth layer of research onion is the final layer which includes two main parts, the data collection and the data analysis. Here on the basis of all the previously made decisions, final selection of the data collection and data analysis techniques and tools are being made. The data collection determine the type of data required as well as the tool which will be used for the collection of that data while the data analysis will determine the technique and tools used for the analysis of the collected data (Palinkas et al., 2015). The process to interpret the data is also being mentioned in the same layer. Moreover, the population, sampling technique and sample size are also defined in this layer.

3.7.1 Data Collection

There are two main types of data that can be collected for any research, whereas both types of data can be collected in single research or if there is need for only one then the choice can be made accordingly. The choice is required to be made between; Primary Data and Secondary Data. The primary data is the fresh data which is collected first hand through direct interaction with the audiences (Silverman, 2018). The secondary data is one which has been published previously on the internet or other mediums and is available for the whole world (sometimes on some conditions like copy rights etc.). For this particular study Primary Data is being concerned for this research and so the research will be based on first hand data collected directly from the participants of the research.

Data to be collected is selected to be primary so in this regard the data collection source is also required to be determined. The population for this paper are the people of the UAE who are using social media sites (almost everyone is using social networking) and the impact about the privacy laws on these social networking websites. However not everyone can be surveyed so a particular amount of representatives from that population will be selected and focused for the study (Chang & Seibert, 2016). Thus, sample size for the study is 300 while the sampling technique used for attaining this number of participants is Random Sampling which is purest probability sampling form.

For the collection of data survey is incorporated and to conduct the survey questionnaire will be used. The questionnaire is designed on the basis of pre-determined MRQs and consists of almost 15 to 20 questions. The questionnaire is closed ended and Likert Scale is used for the responses as responded are provided with five options to choose from, in order to provide the clear insight.

3.7.2 Data Analysis

The final step for the research methodology is data analysis, while since the study is based on quantitative research method so quantities and numerical data is collected that is required to be calculated and measured appropriately using Statistical Data Analysis. In this regard, data is being presented in the form of graphs and charts which is being discussed and interpreted statistically and descriptively (Sandelowski, 2000). Then finally the results are being determined in the form of findings providing justification for the approval or rejection of the MRQs and core aim of the research. The research providing proper solution with ample evidences is considered to be a successful research which can only be successful when the research methodology is designed properly.

Chapter 4. Data Analysis and Interpretation

4.1 Introduction

This chapter summarizes overall data in SPSS file and analyses it with using statistical calculations. The data analyzed in this chapter was taken from 300 networking websites users in the UAE. Statistical test for calculating frequency, percentages, mean and SD are descriptive tests which measure the impact on the regression test performed.

4.2 Reliability of the Questionnaire

The reliability of data is a measure of internal consistency determined to examine the similarity of results. Hence, to measure the internal consistency of 15 questions Cronbach alpha is calculated, that results in a value of 0.86. The value greater than 0.8 is considered as markers of good internal consistency so a questionnaire was measured as having good reliability.

4.3 Quantitative analysis

4.3.1 Demographics

4.3.1.1 Age Group

Majority of the networking web users belonged to the age category of 41-50 that is 31.5%, while other participants were marked 6 %, who were less than 20 years, 25 % were of age 20 to 30 years, 19 % are 31-40 years and 18 % belonged to above 50 years.

Age Group	Frequency	Percentage
<20	19	6%
20-30	74	25%
31-40	58	19%
41-50	94	31%
Above 50	55	18%
Total	300	100%

Table 1 Web user's participant age

4.3.1.2 Gender

It has been determined that networking web users who participated in the study were 56 % males and 44 % female.

Gender	Frequency	Percentage
Male	168	56%
Female	132	44%
Total	**300**	**100%**

Table 2 Web user's participant gender

4.3.1.3 Profession

The profession of the users was included in the questionnaire as to have an idea about the professional status and privacy concerns. From overall data, 12 % were teachers, 33 % lawyers, 32 % doctors, 9 % businessmen/women and 15 % had other professions.

Profession	**Frequency**	**Percentage**
Teacher	36	12%
Lawyer	98	33%
Doctors	95	32%
Business person	26	9%
Others	45	15%
Total	**300**	**100%**

Table 3 Web user's participant profession

4.3.1.4 Internet usage

The time period from which the users have started availing social media networking sites were also included in the questionnaire. Data revealed that 11% were using internet from less than one year, 21% were using from 1 to 3 years, 22% were consuming from 4 to 5 years, 24% were using from 7 to 10 years and 22% were consuming from more than 10 years.

Internet Usage	**Frequency**	**Percentage**
Less than one year	34	11%
1-3 years	63	21%
4-6 years	65	22%
7-10 years	71	24%
more than 10 years	67	22%
Total	**300**	**100%**

Table 4 Web user's participant internet usage

Demographics data was summarized by calculating mean, median, standard deviation and variance as shown in the below table. It represented that demographics have deviation in age (mean=3.3 and SD=1.207), gender (mean=1.44 and SD 0.497), profession (mean=2.82 and SD=1.210) and internet usage (mean=3.24 and SD=1.31).

Statistics					
		Age	**Gender**	**Profession**	**Internet Usage**
N	Valid	300	300	300	300
	Missing	0	0	0	0
Mean		3.3067	1.4400	2.8200	3.2467
Median		3.0000	1.0000	3.0000	3.0000
Std. Deviation		1.20726	.49722	1.21071	1.31844
Variance		1.457	.247	1.466	1.738
Sum		992.00	432.00	846.00	974.00

Table 5 Mean, Median, Standard Deviation and Variance

4.3.2 Descriptive statistics

4.3.2.1 Social networking sites

The descriptive statistics showed in the below table represents that 60% of users have positive views that the UAE considers that GDPR privacy laws are important for social media networking sites as they are offering increased and strict privacies. However, there were 26 % who did not agree with the statement and 14 % have a neutral view. Users presented 54% positive perspective regarding the statement that all social networking sites follows the GDPR privacy laws to manage user information. This statement has a

37% negative perspective and 10% neutral opinion, it means that maybe there are some networking sites offering privacies while others are not. Users take privacy seriously, this got 72% positive answers that they only make an account on those sites, which guarantee privacy. Besides that, there were 21 % users who do not take privacy on serious note whereas 8 % showed neutral answers. In addition, to that 70% of participants were in agreement that when they felt the threat of information steal, they deactivated their accounts. 18 % of participants disagreed with that means that they did not deactivate accounts. The below bar graph in this category showed that account privacy is the major concern of users while using social media networking sites with greater bar.

	Strongly agreed	**Agreed**	**Neutral**	**Disagreed**	**Strongly disagreed**	**Percentage**
The UAE social media sites offering privacy for users.	94	87	41	39	39	300
	31%	29%	14%	13%	13%	100%
All social networking websites follow the GDPR privacy laws to manage user information.	83	79	29	65	44	300
	28%	26%	10%	22%	15%	100%
I have an account on only those social sites which	113	101	25	41	20	300
	38%	34%	8%	14%	7%	100%

guarantee private information protection.						
Whenever I feel threatened about information steal from social media I delete or deactivate my account.	107	102	39	35	17	300
	36%	34%	13%	12%	6%	100%

Table 6 Descriptive statistics of social networking sites

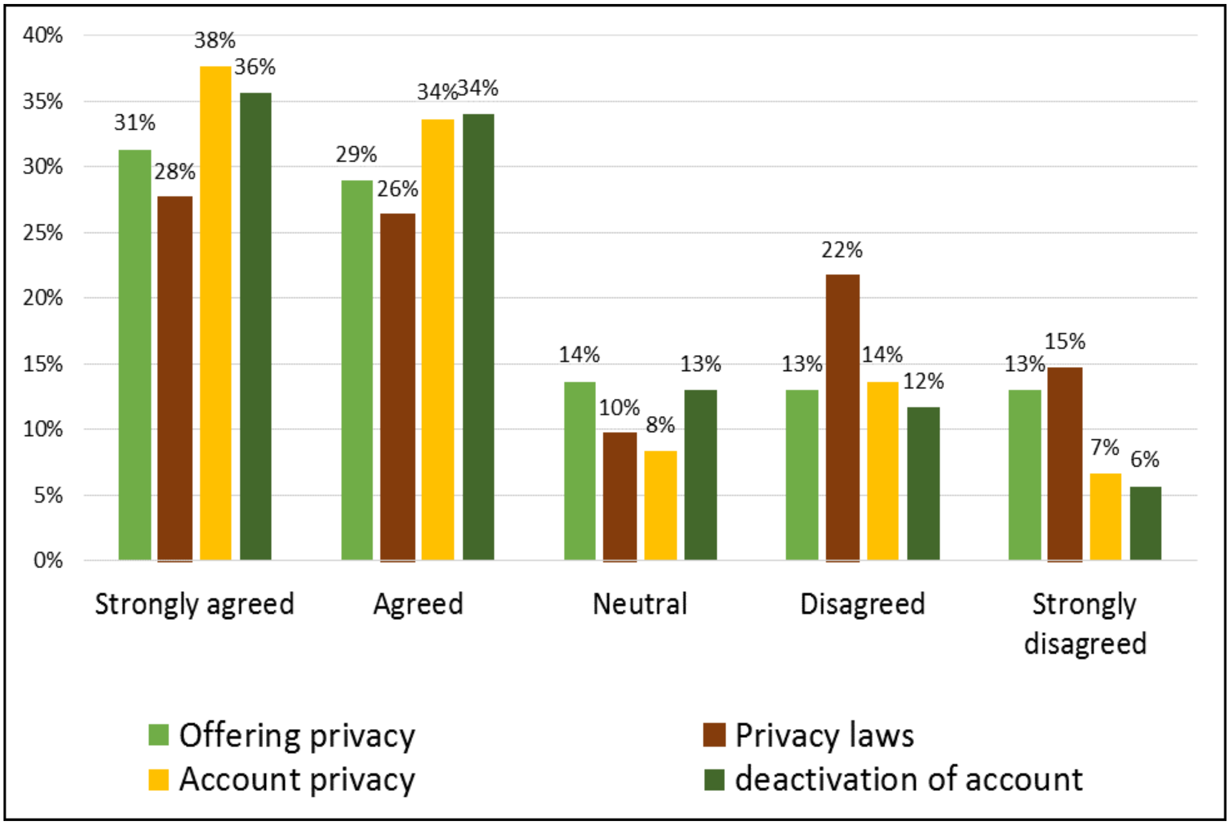

Figure 3 Graphical presentation of social networking sites

4.3.2.2 Personal information policies

It is the first category under the independent variable of privacy laws in which four questions were included to measure the impact of privacy laws on social networking websites by users. There are 79% positive answers for the statement that users get bothered when social networking sites ask them regarding personal information. Only 7 % participants showed negative perception with these concerns shows that majority of user’s shows bothering behavior. Along with that, 74% of users mentioned that submitting personal information on social networking sites is a threat. Again, few participants 17% marked disagreed and strongly disagreed options for this statement. 72% participants presented a positive review that whenever social networking sites ask for personal information such as age, gender, birth their privacy concerns increases. However, 18 % of social networking, users had a negative opinion and 11 % were neutral in this regard. 78% users illustrated that they prefer those networking sites, which follows GDPR and does not ask for personal information. Nevertheless, 11 % presented negative perceptions by making disagree and strongly disagree and 11 % remains neutral. The bars in the below graph are representing that from all personal information questions the majority of the answers lie in between strongly agreed and agreed.

	Strongly agreed	Agreed	Neutral	Disagreed	Strongly disagreed	Percentage
It bothered me when social media websites ask about personal information.	131	106	29	22	12	300
	44%	35%	10%	7%	4%	100%
I believed that submitting personal information is a threat.	142	81	25	37	15	300
	47%	27%	8%	12%	5%	100%
UAE social media websites ask for name, age, birth, and gender which always increase my privacy concerns.	126	90	32	23	29	300
	42%	30%	11%	8%	10%	100%
I select those networking sites, which follows GDPR, and do not ask about personal information.	129	105	33	16	17	300
	43%	35%	11%	5%	6%	100%

Table 7 Descriptive statistics of Personal information policies

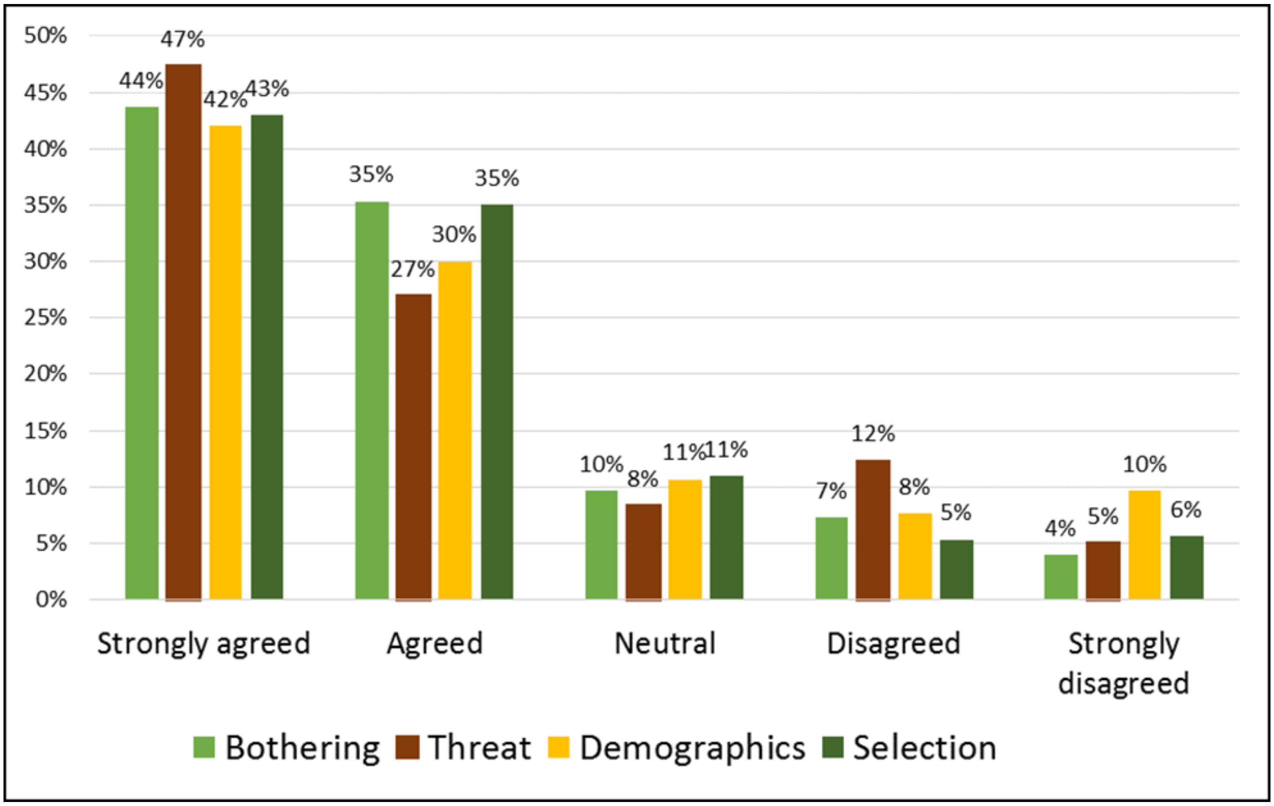

Figure 4 Graphical presentation of personal information policies

4.3.2.3 Control and notification

Another privacy concern is the control and notification system on social networking sites followed in the UAE. It was measured with 76% positive answers that the user accepts those social networking sites, which give them control over private information due to GDPR. However, few 13 % presented negative perceptions by marking disagree and strongly disagree and 12 % remains neutral. Furthermore, users showed a 71% positive agreement that complete control over personalized communication was found to be an attractive feature that enables them to engage on social networking site. However, 17 % presented negative perceptions by making disagree and strongly disagree and 12 %

remains neutral. Notification is also an acceptance privacy concerns agreed by 70% users as it makes them aware of what happens. Although 22% showed negative, reviews and 8 % of users have a neutral opinion regarding that. 77% of users presented a positive perspective that they are concerned about notifications because it notifies them about the interruptions. However, very few 14 % of social networking users had a negative opinion and 10 % were neutral in this regard. The graphical presentation for control and notification shows that this privacy concern has an impact on social networking acceptance.

	Strongly agreed	**Agreed**	**Neutral**	**Disagreed**	**Strongly disagreed**	**Percentage**
I prefer those UAE social media sites, which give me control over my private information due to GDPR.	119	108	36	23	14	300
	40%	36%	12%	8%	5%	100%
Control on personalised communication laws always attracts me to get engaged on websites.	108	106	36	29	21	300
	36%	35%	12%	10%	7%	100%
The notification features notify me of what is happening around.	112	100	23	35	30	300
	37%	33%	8%	12%	10%	100%
I accept notification feature because it notifies me about the interruptions that occur on my private data.	128	101	31	26	14	300
	43%	34%	10%	9%	5%	100%

Table 8 Descriptive statistics of Control and notification

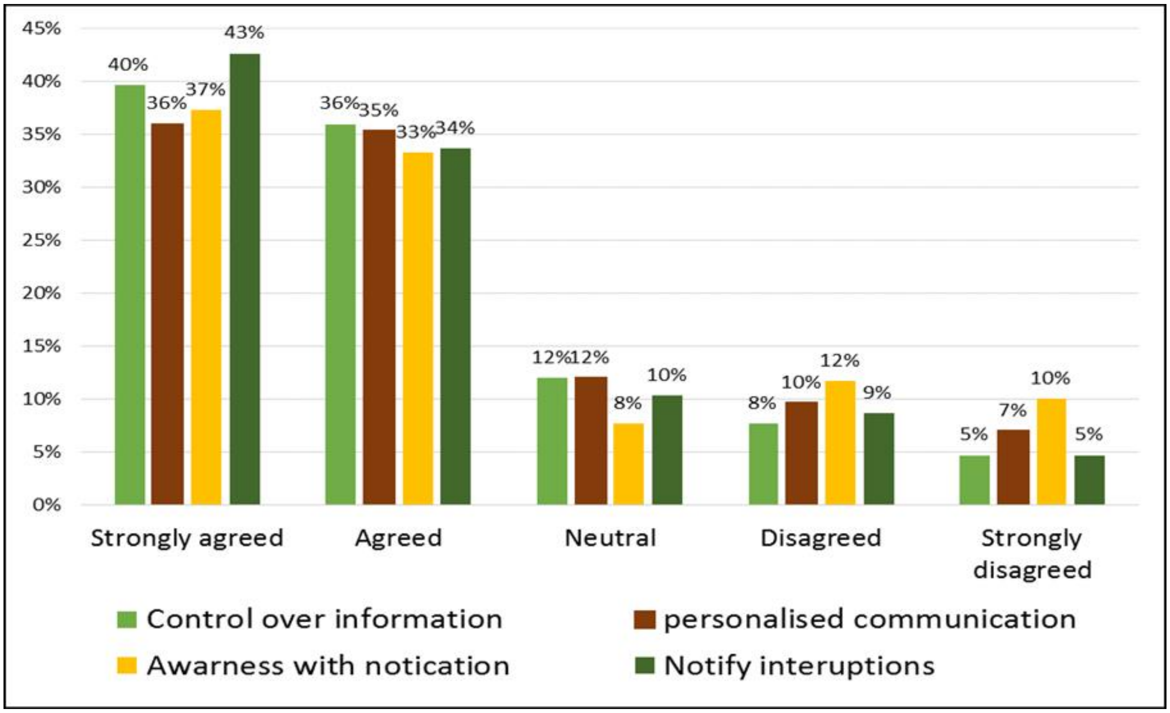

Figure 5 Graphical presentation of control and notification

4.3.2.4 Deleting information policies

UAE internet users also have privacy concerns about the use of deleting their information on social networking sites. It was measured with 81% positive opinions that users accept those social networking sites, which has GDPR because it give access to delete their private information. Few participants i.e.11 % presented negative perceptions by marking disagree and strongly disagree and 8 % remain neutral. Whereas, 66 % of the participants mentioned that they accept those sites, which give access to them and ownership to delete the private information. There were 76% positive views that data deleting as privacy concerns for social networking sites is included the UAE privacy laws. However, 12% of the participants did not agree with this statement. 74% of the users mentioned that they are comfortable with the use of those social networking sites, which provide full authenticity to delete private information whenever needed. Although 14 % of the users showed negative reviews and 11% of social networking users have a neutral opinion regarding that. The graphical representation showed that the majority of users have agreed with all statements on deleting information privacy policies; this means that it has an impact on the user's acceptance. The higher value for the strongly agreed is for privacy laws i.e. 56 % this means that in the UAE users consider deleting as a privacy concern.

	Strongly agreed	**Agreed**	**Neutral**	**Disagreed**	**Strongly disagreed**	**Percentage**
I have an account on those social media websites, which has GDPR because it gives me access to delete my private information.	129	115	23	10	23	300
	43%	38%	8%	3%	8%	100%
Deleting data present in the UAE social media privacy laws.	161	65	18	36	20	300
	54%	22%	6%	12%	7%	100%
I have an account on those social media websites which give access to me and ownership to delete my private information.	93	104	45	41	17	300
	31%	35%	15%	14%	6%	100%
	100	122	34	28	16	300

I am comfortable to use those social sites which provide full control over deleting information whenever needed.	33%	41%	11%	9%	5%	100%

Table 9 Descriptive statistics of deleting information policies

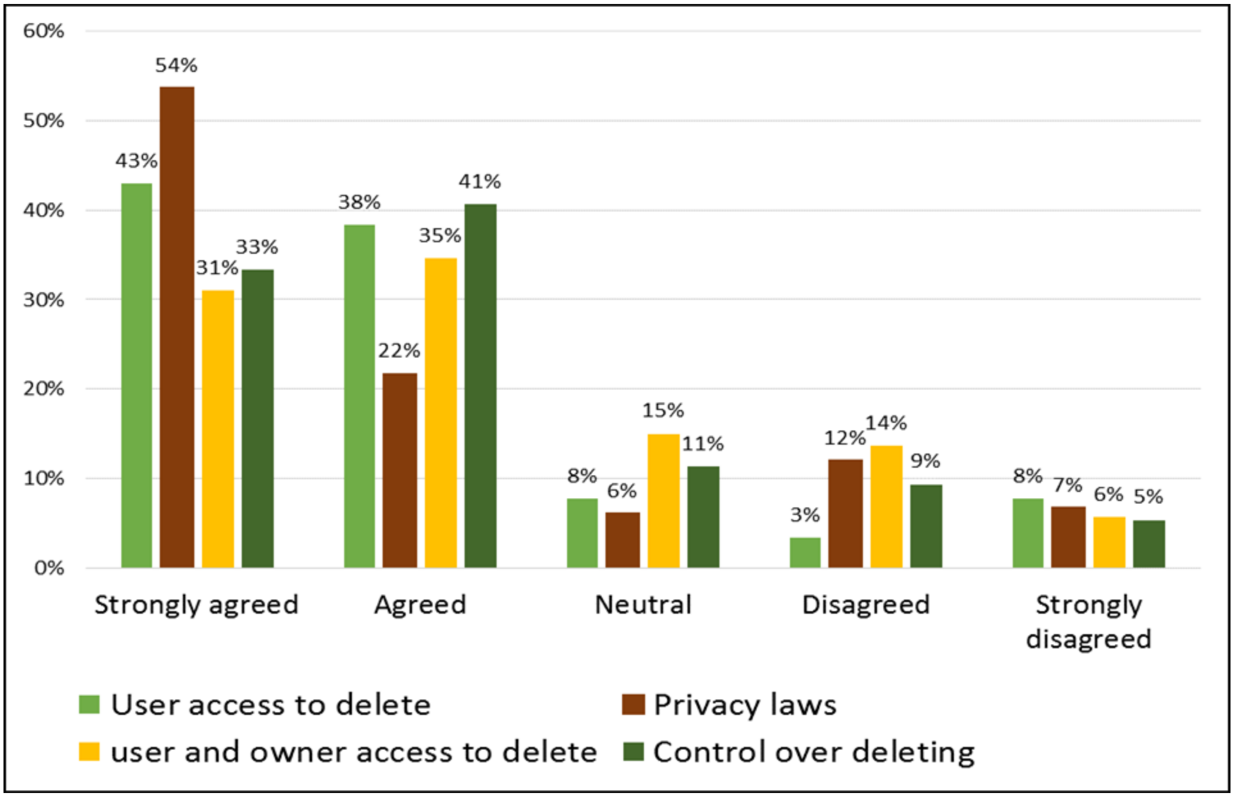

Figure 6 Graphical presentation of deleting information

4.3.2.5 Risk *awareness*

It is the last category to measure the impact of privacy concerns on the user's social networking site acceptances. From the participant's perceptions, it has been examined that 82% of the users believed there is a risk to share private information on social networking sites in the UAE. Though few very 8 % showed negative, reviews and 11 % of social networking user have a neutral opinion regarding that. However, risk awareness privacy laws of GDPR are followed by social networking sites while being accessed from UAE; this was agreed by 84% users. 8% presented negative perceptions by making disagree and strongly disagree and 8 % remains neutral. It shows that risk awareness rules are followed but still users do not have trust on social networking sites. 76% users illustrated that they select social sites based on risk management because there is a chance of private information potential lost. However, 21 % presented negative perceptions by making disagree and strongly disagree and 11 % remains neutral. The bars in the graphs presented that majority of responses lie between strongly agreed and agreed options.

	Strongly agreed	**Agreed**	**Neutral**	**Disagreed**	**Strongly disagreed**	**Percentage**
There is always a risk to share private information on UAE social media sites.	120	125	32	15	8	300
	40%	42%	11%	5%	3%	100%
The risk awareness privacy laws of GDPR are adopted by all the UAE social media sites.	145	108	24	15	8	300
	48%	36%	8%	5%	3%	100%
I choose social sites wisely as there is a chance of potential loss of private information.	124	104	38	13	21	300
	41%	35%	13%	4%	7%	100%

I accept social networking sites that guarantee risk awareness.	129	73	33	43	22	300
	43%	24%	11%	14%	7%	100%

Table 10 Descriptive statistics of risk awareness

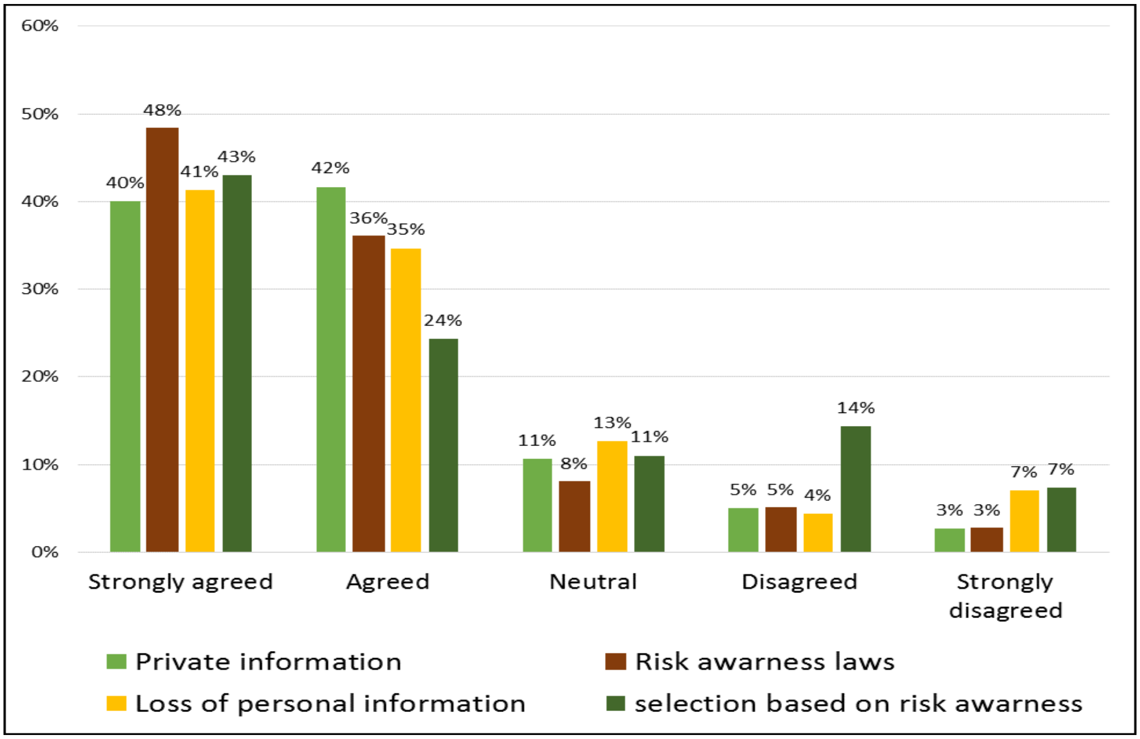

Figure 7 Graphical presentation of risk awareness

4.3.3 Regression

4.3.3.1 Personal information policies

The table contains the impact of users' privacy concerns for personal information policies on their acceptance of social networking websites in the UAE. It has been determined that there is a 68% impact of personal information on to the user's acceptance for social media. R-value 0.827 shows a high degree of correlation between these two variables. The significance value in the ANOVA table presented that the value is extremely low. It is even low than the 0.05, which is the standard value associated with the hypothesis testing. Hence, it is measured as the accepted range means the relationship is significant.

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. The error of the Estimate**
1	.827[a]	.684	.667	9.45218
a. Predictors: (Constant), Personal information policies				

Table 11 Model Summary

ANOVA [b]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	9.868	1	9.868	23.703	.000[a]
	Residual	124.059	298	.416		
	Total	133.927	299			
a. Predictors: (Constant), Personal information policies						

ANOVA [b]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	9.868	1	9.868	23.703	.000[a]
	Residual	124.059	298	.416		
	Total	133.927	299			
b. Dependent Variable: Social media						

Table 12 ANOVA b

4.3.3.2 *Control and Notification*

The below regression table presented that the impact of users' privacy concerns for control and notification on their acceptance of social networking websites in the UAE. From the R square value, it has measured that control and notification privacy laws influenced the user’s social networking acceptance by 45%. R-value of 0.673 shows a moderate level of correlation between notification and social networking acceptance. The ANOVA table presented the significance value of 0.030, which is lesser than the acceptable limits of 0.05, hence the relationship is significant.

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. The error of the Estimate**
1	.673[a]	.453	2.894	.66917
a. Predictors: (Constant), Control And Notification				

Table 13 Model Summary

ANOVA [b]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	.487	1	.487	1.087	.030[a]
	Residual	133.441	298	.448		
	Total	133.927	299			
a. Predictors: (Constant), Control And Notification						
b. Dependent Variable: Social media						

Table 14 ANOVA b

4.3.3.3 Deleting information

The below table presented the impact of deleting information privacy concerns in users on acceptance of social networking websites the UAE. The model summary table presented 0.65 value for R square that demonstrates privacy concerns for deleting information exerts 65% change in acceptance of social media. The R-value 0.807 shows a high degree of correlation in between these two variables. ANOVA table presented extremely low values; this means that relationship is a good fit and significant.

Model Summary

Model	R	R Square	Adjusted R Square	Std. the error of the Estimate
1	.807[a]	.65	.618	.64825

a. Predictors: (Constant), Deleting information

Table 15 Model Summary

ANOVA [b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.700	1	8.700	20.704	.000[a]
	Residual	125.227	298	.420		
	Total	133.927	299			

a. Predictors: (Constant), Deleting information

b. Dependent Variable: Social media

Table 16 ANOVA b

4.3.3.4 Risk awareness

Below tables, represent the impact of risk awareness privacy concerns in users on acceptance of social networking websites in the UAE. R square value of 0.61 showed that risk awareness caused a 61% change in acceptance of social networking websites. R-value 0.780 presents good correlations between risk awareness privacy concerns and users' acceptance. Moreover, ANOVA presented significant value less than 0.05, which is acceptance range.

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. the error of the Estimate**
1	.780[a]	.61	.416	.61217
a. Predictors: (Constant), Risk awareness				

Table 17 Model Summary

ANOVA [b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	22.253	1	22.253	59.381	.000[a]
	Residual	111.675	298	.375		
	Total	133.927	299			

a. Predictors: (Constant), Risk awareness

b. Dependent Variable: Social media

Table 18 *ANOVA b*

Chapter 5. Recommendations and Conclusions

5.1 Discussion of findings

This study has empirically tested privacy concerns and GDPR laws for measuring the user’s acceptance of social networking sites in the UAE. The statistical test confirms that there is an impact on users' privacy concerns on their acceptance of social networking websites in the UAE. This impact has been determined by measuring privacy concerns with personal information policies, risk awareness, control and notification and deleting information. Personal information factors deal with all users concerns based on sharing personal information on social networking sites. Risk awareness measures the risk of data loss and users concerns for privacy laws based on risk. Control and notifications determine the user’s acceptable behavior for social networking sites regarding regulating information along with alarming alert. Deleting information included the details of user’s acceptance behavior regarding deleting features in social networking account. It has been demonstrated that social networking sites are the channels for communication and building a professional or personal relationship amongst individuals.

The demographics information shows that the internet is used by the people of almost every age group from less than 20 to 50. Similarly, Lenhart, Purcell, Smith and Zickuhr (2010), demonstrated that internet is used mostly by teenagers, young and adults. Gender examination presented that both male and female use social networking sites at an almost equal ratio. A study by Vishkaie and Elssa (2016) also showed in the demographic profile that both genders male and female use the internet. The profession of the internet users was also examined as to estimate their perceptions and concerns based on career. Results showed that professions of the majority of the participants were teachers, lawyers, doctors, businessmen/women, and others. These professions were included because Itani, Sidani and Baalbaki (2011), presented that these are the common professions in the UAE. Use of the internet for social networking is common because in the study it examines that users are consuming social networking sites from less than one year to more than 10 years. Similarly, the study by Dunne, Lawlor and Rowley (2010), explored that social networking is found to be a common medium for the people to communicate and connect with the world around. The results of this show larger variations in usage maybe it is due to the difference in age groups or profession of the participants.

In context to the social networking sites, it has been measured with the results of a study that UAE websites offers GDPR privacy for their users. This result could be backed up with the findings in a study by Saleh et al., (2011), who illustrated that the UAE takes social networking websites very seriously as they never reveal the identity of individuals. This means that maybe the UAE agencies that manage social networking sites through GDPR are concerned about user’s privacy and take it seriously. However, these results contradict with the results by Kuzma (2011), who examined that there are certain privacy issues on social networking UAE websites due to unannounced changes in privacy laws. Furthermore, results examined that social networking privacy laws are followed by UAE social networking websites but not by all. Results regarding privacy laws show that maybe there are some websites which are concerned about privacy but do not have to abide by privacy laws. Christian (2011), referred that are challenges in notion to develop privacy laws due to advance liberal privacy concept.

The user's perception illustrated that they prefer to make an account on those social sites which offer GDPR or guarantee the privacy of information. Similarly, a study by Kosta, Kalloniatis, Mitrou and Gritzalis (2010), analyzed that privacy on social networking increases user interaction and collaborations. It means that may be with personal information privacy legislation users feel secure and feel connected with social networks. This result shows the impact of privacy concerns because the user's behavior to choose social networking sites depends upon privacy laws. The results of this study further examined that whenever the user feels threatened or senses that private information would be stolen they delete or deactivate their accounts. Research by Feng and Xie (2014) also shows similar results that users have deleted accounts and take it as personal protection. It may be because users do not trust the UAE social networking or feel that their information would be misused. These results could be backed up with the results of Steeves and Regan (2014), who measured that social actors have a poor concept for the privacies because they do not trust networking sites. This result further supports the above statement that privacy laws influenced the acceptance of social media networking sites by the users.

The first measures for determining the privacy concerns impact on user's acceptance for social networking sites are personal information policies. Results have determined that when social networking sites ask about personal information the users get bothered. A similar result was obtained by findings of Benson, Saridakis, and Tennakoon (2015), which examined sharing personal information is a bothering factor because the control over private data is lost. Irritation and trouble may occur because users do not want to disclose their confidential information, or they have ethical concerns. Smahel, Wright and Cernikova (2014), referred that personal information sharing is taken as a problematic situation by users as they do not want to enter personal life on social networks. The reason for feeling bothered can also be examined with the users who believed that submitting personal information is a threat. This threat factor was also examined by Ziegeldorf, Morchon and Wehrle (2014), who mentioned that threat is involved in online social networking, as there are smart tracking software's available to attack networks.

The study also measured the user's increasing privacy concerns when social networking sites ask for demographic information such as age, gender, name, and birth. Similarly Kosta, Kalloniatis, Mitrou and Gritzalis (2010), users have data protection issues while entering private details on social networking sites. This may be because they are not familiar with the privacy laws or do not know how features get applicable and not account. Results revealed that the users accept those social networking sites, which do not ask about personal information. Furthermore, results demonstrated the impact of users' privacy concerns for personal information policies on their acceptance of social networking websites in the UAE. Research by Benson, Saridakis and Tennakoon (2015), also determined the significant impact of privacy concerns and social networking context.

The second privacy concerns included in the study is control and notification to measure the acceptance of social networking websites by users. Results measured that GDPR privacy laws and concerns for control and notification affected the user's acceptable behaviour. Notification as privacy concern was also measured by Vishkaie and Elssa (2016), in the study it has been examined that the users believed notification through any medium such as email gives awareness. It is maybe because users feel active and feel that the UAE social networking sites give them privacy protection. The research examined that the UAE social networking users prefer those websites, which give them control over private information. These results could be backed up with the results of Fuchs (2011), who illustrated that privacy naturalistic approach was selected because individuals want to control and structure privacy. This means that privacy control laws influence the users' approach to accept the social networking websites of UAE.

It was also measured that personalized communication laws of GDPR attract users to get engaged on websites. Communication personalization results were found to be similar with findings by Aguirre, Roggeveen, Grewal and Wetzels (2016), which argued that personalization communication on social websites might enhance or diminish user's acceptance. This result shows personalized communication laws must adapt but there must be a balance to process information. Social networking acceptance is also influenced by notification, as users prefer those websites that have notification feature because it notifies them of what is happening around. Similarly, results by Vishkaie and Elssa (2016), demonstrated that notification on social networking websites is a good feature to provide awareness regarding any sort of information. User's perceptions regarding notification features can be examined with the results that it gives an alarming alert for interruptions that happen on accounts. Dunne, Lawlor and Rowley (2010), results showed similarity with findings that notification makes user synchronize and be physically active.

Users’ concerns regarding control and notification for social networking may be because the personal social account contains their private data. Thus, it determines that there is an impact of users' privacy concerns for control and notification on their acceptance of social networking websites in the UAE.

Further, the research included deleting information policy in GDPR privacy concern to measure the user’s social networking acceptance. It was measured that users prefer to make an account on those social sites that give them access to delete private information. Similarly, a study by Vishkaie, and Elssa (2016), revealed that the users should be given an option to delete the information from social networking account at any time. It may because the threat of information misuse can occur at any time. However, other individuals showed satisfaction with those websites that give deleting information access to users and company owners. This result shows similarity with the results by Feng and Xie (2014) that demonstrates to modify or delete account information should only be on user’s ends. The point to notice here is that common consideration in both of these findings is deleting access at user’s ends. Results revealed that deleting data on social networking sites is present in the UAE privacy laws. Research also analyzed that the users comfortably use those social networking sites that give them control over deleting information whenever they want. It may be because the users can easily delete private data when observing any threat or can delete information whenever they want.

The last measure for privacy concern is GDPR risk awareness policy in determining social networking acceptance by users. Risk factors as privacy concerns are also highlighted by Kosta, Kalloniatis, Mitrou and Gritzalis (2010), who demonstrated that there is always a privacy risk on social networking. Results revealed that the users believed that there is a risk associated with sharing personal or private information on social networking sites may be due to the misuse of information. However, it has been determined that risk awareness privacy laws are adopted by all the UAE social networking sites. The research examined that users select social sites wisely because they believed that there is a potential loss of private data. Similarly, Feng and Xie (2014), examined the risk of privacy data loss on voluntarily or involuntarily basis on social websites. Further, the research examined that users accept those social networking sites, which guarantee them about risk awareness. The research illustrated that there is an impact of privacy concerns for risk awareness on social acceptance of users the UAE.

5.2 Implications

Through wrapping up the findings of this study, this section explains the implications of results on a practical level. The implication can be explained based on the determined impact of privacy laws or concerns on user’s acceptance for social networking sites in the UAE. In this essence, the users were confident that they take privacy at a serious level because there is always a threat of crime or stealing of data. When it comes to practical application for this notion, it regards that the UAE should take serious notice for the privacy concerns. The General data protection regulation must need to monitor privacy so that the users build trust in using social networking sites. Government UK (2018), referred that for any medium that uses personal data must abide by certain rules which are transparency, lawfulness, fairness, accurate handling and give legal protection.

It has been determined that there is always a threat associated with sharing personal information and user's acceptance with social websites depends upon these privacy concerns. Therefore, the UAE authorities must follow such measures that guarantee the protection of sensitive information and other personal details. This is necessary, as in accordance with research by Aguirre, Roggeveen, Grewal and Wetzels (2016), who investigated that personalization privacy is important for digital social media networks. However, the study focused on personal information as privacy concerns but did not focus on user's acceptance based on sensitive information. If the social networking sites guarantee the protection of users, maybe then bothering and issues with sharing demographics will be diminished. Moreover, this implication is designed in accordance with Fuchs (2011) study, in which legislation to follow the privacy has been founded. The author identified that all social networking sites that provide privacy, increases the connection with people.

There must a control and notification feature on every social media site because the user's perceptions to select websites depend upon that. According to Vishkaie and Elssa (2016), when the user gets a notification through email about an activity on the social account, they can check and respond to any issue immediately. Furthermore, this is important because the chance of attack or stealing of personal information on the social account is always present. Another important concern is the deleting of information whenever required by the users. This implication is made with a study by Feng and Xie (2014), who determined that deleting information should be present at users end. By providing access to the user for deleting of information in future may end the complaints regarding the information misuse. Further, the research gives arguments to adopt the risk awareness policies so that users can be notified of what happens on social sites. Dunne, Lawlor and Rowley (2010), identified that in certain cases users do not have the knowledge regarding the risk and how to use social networking features. Therefore, in this case whenever new features launch the knowledge to use must be transferred to the users.

Appendixes A – References

1. Millar, S. (2006). Privacy and security: Best practices for global security. Journal Of International Trade Law And Policy, 5(1), 36-49. doi: 10.1108/14770020680000539
2. Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users. Information Technology & People, 28(3), 426-441. doi: 10.1108/itp-10-2014-0232
3. Aguirre, E., Roggeveen, A., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. Journal of Consumer Marketing, 33(2), 98-110. doi: 10.1108/jcm-06-2015-1458
4. Fuchs, C. (2011). Towards an alternative concept of privacy. Journal of Information, Communication and Ethics in Society, 9(4), 220-237. doi: 10.1108/14779961111191039
5. Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. Journal of Information, Communication and Ethics in Society, 12(4), 298-313. doi: 10.1108/jices-01-2014-0004
6. Kosta, E., Kalloniatis, C., Mitrou, L., & Gritzalis, S. (2010). Data protection issues pertaining to social networking under EU law. Transforming Government: People, Process and Policy, 4(2), 193-201. doi: 10.1108/17506161011047406
7. Pierson, J., & Heyman, R. (2011). Social media and cookies: challenges for online privacy. Info, 13(6), 30-42. doi: 10.1108/14636691111174243

8. Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. Online Social Networks And Media, 3-4, 1-21. doi: 10.1016/j.osnem.2017.09.001

9. Van Audenhove, L., Constantelou, A., & Poel, M. (2011). Online content: European policy and regulation in a global market. Info, 13(6). doi: 10.1108/info.2011.27213faa.001

10. Biesta, G. (2015). On the two cultures of educational research, and how we might move ahead: Reconsidering the ontology, axiology and praxeology of education. European Educational Research Journal, 14(1), 11-22.

11. Chang, W., & Seibert, J. H. (2016). U.S. Patent No. 9,262,250. Washington, DC: U.S. Patent and Trademark Office.

12. Howes, L. M. (2017). Developing the methodology for an applied, interdisciplinary research project: Documenting the journey toward philosophical clarity. Journal of Mixed Methods Research, 11(4), 450-468.

13. Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. International Journal of Project Management, 34(6), 1043-1056.

14. Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533-544.

15. Quinlan, C., Babin, B., Carr, J., & Griffin, M. (2018). Business research methods. South Western Cengage.

16. Sandelowski, M. (2000). Combining qualitative and quantitative sampling, data collection, and analysis techniques in mixed-method studies. Research in nursing & health, 23(3), 246-255.

17. Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

18. Silverman, B. W. (2018). Density estimation for statistics and data analysis. Routledge.

19. Singh, K. D. (2015). Creating your own qualitative research approach: Selecting, integrating and operationalizing philosophy, methodology and methods. Vision, 19(2), 132-146.

20. Smarandache, F. (2016). Administration, Teaching and Research Philosophies.

21. Soy, S. (2015). The case study as a research method.

22. Vamsi Krishna Jasti, N., & Kodali, R. (2014). A literature review of empirical research methodology in lean manufacturing. International Journal of Operations & Production Management, 34(8), 1080-1122.

23. Aguirre, E., Roggeveen, A., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. Journal of Consumer Marketing, 33(2), 98-110. doi: 10.1108/jcm-06-2015-1458

24. Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users. Information Technology & People, 28(3), 426-441. doi: 10.1108/itp-10-2014-0232

25. Dunne, Á., Lawlor, M. A., & Rowley, J. (2010). Young people's use of online social networking sites–a uses and gratifications perspective. Journal of Research in Interactive Marketing, 4(1), 46-58. DOI 10.1108/17505931011033551

26. Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior, 33, 153-162. doi.org/10.1016/j.chb.2014.01.009

27. Fuchs, C. (2011). Towards an alternative concept of privacy. Journal of Information, Communication and Ethics in Society, 9(4), 220-237. doi: 10.1108/14779961111191039

28. Itani, H., Sidani, Y. M., & Baalbaki, I. (2011). United Arab Emirates female entrepreneurs: motivations and frustrations. Equality, Diversity and Inclusion: An International Journal, 30(5), 409-424.

29. Kosta, E., Kalloniatis, C., Mitrou, L., & Gritzalis, S. (2010). Data protection issues pertaining to social networking under EU law. Transforming Government: People, Process and Policy, 4(2), 193-201. doi: 10.1108/17506161011047406

30. Kuzma, J. (2011). Empirical study of privacy issues among social networking sites. J. Int'l Com. L. & Tech., 6, 74. Doi: 1053/2/privacyconferencenov2010rev1

31. Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. Pew internet & American life project. 1-36 doi: ED525056

32. Saleh, F., Jani, H., Al Marzouqi, M., Al Khajeh, N., & Rajan, A. (2011). Social networking by the youth in the UAE: A privacy paradox. In Current Trends in

Information Technology (CTIT), 2011 International Conference and Workshop on (pp. 28-31). IEEE. DOI: 10.1109/CTIT.2011.6107957

33. Smahel, D., Wright, M. F., & Cernikova, M. (2014). Classification of online problematic situations in the context of youths' development. Communications, 39(3), 233-260. Retrieved 11-November'2018from https://www.researchgate.net/profile/David_Smahel/publication/264627033_Classification_of_online_problematic_situations_in_the_context_of_youths'_development/links/53e9e98a0cf2fb1b9b67429a.pdf
34. Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. Journal of Information, Communication and Ethics in Society, 12(4), 298-313. doi: 10.1108/jices-01-2014-0004
35. Vishkaie, M., & Elssa, S. (2016). A Qualitative Inquiry into Online Privacy and Information Sharing Concerns of Internet Users. Master Thesis in Informatics. 1. 1-56 doi: smash/get/diva2:922604/FULLTEXT01
36. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742. DOI: 10.1002/sec.795
37. Government UK, (2018). Data protection. Retrieved 11-November'2018from https://www.gov.uk/data-protection

Appendixes B – Research Questionnaire

A. Introduction

This questionnaire will aid us in conducting a research which shows a relationship between impact of privacy laws on social media.

Please do not write your name or any personal identification details. This questionnaire is solely conducted for academic purposes.

B. Demographics

Age Bracket	Gender	Profession	Internet Usage
○ < 20 ○ 20 – 30 ○ 31 – 40 ○ 41 - 50 ○ Above 50	○ Male ○ Female	○ Teacher ○ Lawyer ○ Doctor ○ Business Person ○ Others	○ Less than 1 year ○ 1 – 3 years ○ 4 – 6 years ○ 7 – 10 years ○ > 10 years

C. Social networking sites

Question	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
The UAE social media sites offering privacy for users.	○	○	○	○	○
All social networking websites follow the GDPR privacy laws to manage user information.	○	○	○	○	○

I have an account on only those social sides which guarantee private information protection.	○	○	○	○	○
Whenever I feel threatened about information steal from social media I delete or deactivate my account.	○	○	○	○	○

D. Personal information policies

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It bothered me when social media websites ask about personal information.	○	○	○	○	○
I believed that submitting personal information is a threat.	○	○	○	○	○
I select those networking sites, which follows GDPR, and do not ask about personal information.	○	○	○	○	○
UAE social media websites ask for name, age, birth, and gender which always increase my privacy concerns.	○	○	○	○	○

E. Social networking sites

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I prefer those UAE social media sites, which give me control over my private information due to GDPR.	○	○	○	○	○
Control on personalized communication laws always attracts me to get engaged on websites.	○	○	○	○	○
The notification features notify me of what is happening around.	○	○	○	○	○
I accept notification feature because it notifies me about the interruptions that occur on my private data.	○	○	○	○	○

F. Deleting information policies

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have an account on those social media websites, which has GDPR because it give me access to delete my private information.	○	○	○	○	○
Deleting data present in the UAE social media privacy laws.	○	○	○	○	○
I have an account on those social media websites which give access to me and ownership to delete my private information.	○	○	○	○	○
I am comfortable to use those social sites which provide full control over deleting information whenever needed.	○	○	○	○	○

G. Risk awareness

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
There is always a risk to share private information on UAE social media sites.	○	○	○	○	○
The risk awareness privacy laws of GDPR are adopted by all the UAE social media sites.	○	○	○	○	○
I choose social sites wisely as there is a chance of potential loss of private information.	○	○	○	○	○
I accept social networking sites that guarantee risk awareness.	○	○	○	○	○