Research Article

Global Media Journal
ISSN 1550-7521

2023
Vol.21 No.66:400

Influence of Social Media on Modern Day Political Culture and Policy Building

S Sultan*

Media and Communication Studies, Institute for Art and Culture, India

Abstract

In the modern era of advancement internet emerged to be the most influential source for connecting people. With the innovation and advancement in technology, Social Networking Sites (SNS) are progressing and they appeared to be the most powerful and modern tool for connecting individuals across the globe. The usage of social sites is expanding at a swift pace and this century could be considered as the thriving period for social networking. The concerns for privacy on social media have soared high in recent years. Incidents concerning data breaches have agitated many users and prompted them to reconsider their personal relationships to social media and about the security of their personal data. Moreover, it has been noted that attack or issue against any online social site usually spread rapidly than other kinds of online attacks the reason being the trust that exist between the users of these network. There are several methods that could be done to contemplate or grasp the concept of social media and its impact. The major portion of this research is written on the basis of information taken from secondary qualitative sources such as reports, books, websites, press articles and analyses based on political researches, therefore using a qualitative methodology. This study will help understand and extract the online privacy concerns of the users (from the published literature) to get a better idea of domains, questions, and issues around which to anchor the intended objectives of the study. This has been achieved by performing an in-depth literature review.

Keywords: Political communication; Agenda setting; Public opinion making; Digital content impacts

***Corresponding author:**
S Sultan

sultan@gmail.com

Assistant Professor Media and Communication Studies, Institute for Art and Culture, India

Citation: Sultan S (2023) Influence of Social Media on Modern Day Political Culture and Policy Building. Global Media Journal, 21:66.

Received: 18-Oct-2023; Manuscript No. gmj-23-117346; **Editor assigned:** 21-Oct-2023; Preqc No. gmj-23-117346; **Reviewed:** 07-Nov-2023; QC No. gmj-23-117346; **Revised:** 15-Nov-2023; Manuscript No. gmj-23-117346 (R); **Published:** 01-Dec-2023, DOI: 10.36648/1550-7521.21.66.400

Introduction

In the modern era of advancement internet emerged to be the most influential source for connecting people. With the innovation and advancement in technology, Social Networking Sites (SNS) are progressing, and they appeared to be the most powerful and modern tool for connecting individuals across the globe [1]. These networking sites have shaped international, transnational, and national groups where strange individuals can meet and form a social bond. Among the most prominent SNS, Facebook, Skype, WhatsApp, Myspace, and Viber have made their way to the top tier. These applications have made the life easier by attracting and connecting people from different parts of the world, plenty of them has incorporated these into their daily practices. These SNS have altered the way people connect across the globe.

Due to this tendency of social media of connecting people, the usage of social sites is expanding at a swift pace and this century could be considered as the thriving period for social networking. Over this past decade, social media usage has increased exponentially and this increase has made it the most powerful and popular services of internet in the world, building new approaches to “see and be seen” [2]. Social media usage has altered communication landscape which subsequently resulted in changed behavior and ethical norms. This unprecedented increase in the usage has caused reduction in usage of any other media and also adversely affecting safety, privacy, political and civic engagement.

In February 2019, a report was submitted by Smart Insights stating that over 3.484 billion people use social media platforms. This report further indicates that the rate by which individuals are using social media is increasing 9% annually and this trend is

assumed to continue in future. At present, approximately 45% of the total world population is using social media. The most frequent users of these sites are "digital natives"; this term is used for those individuals who have been born or grown in this era of digital advancement and are more acquainted with numerous innovations and systems, and those who became adult at the end of twenty century, generally termed as "Millennial Generation". These users tend to utilize the platform of social media for numerous purposes ranging from health care, marketing, civic engagement, news acquisition, politicking, coaching, and social engagement. Pew trust conducted a study which stated that 80% people who use social media are concerned about their business ventures and observe advertisers reading and using their posts on social media. In 2019, reports revealed that kids aged between 8 and 11 years on average devote 13.5 hours per week online and 18% of this age group actively uses social media. Those individuals whose age range between 12 and 15 devote 20.5 hours online and 69% of these individuals actively engage on social media.

A company named Alexa monitored the traffic on the net, it shows that Twitter, Facebook and YouTube ranks among top four most frequently visited platforms up till August 2019 and Google being the most used search engine even exceeding all social media platforms. Social media platforms/sites can be best described as services that exist online allowing users to make their profiles which can be changed to either "semi-public", "public" or both. Users can also make individual profiles and they can also be a part of groups with whom he/she may have relationships or acquaintance offline [3]. There are many facilities provided by these social sites to make communication easier. These facilities includes blogs, chat rooms, public comments, private messages, sharing photos and videos and ways of sending content that is external to the site. However, these facilities also bring along numerous consequences for instance breach of privacy and cyber related crimes.

Since teenagers and children represent largest user group, most of the time they don't know how to properly protect information on the internet and they are mostly vulnerable to the cyber related crimes mostly breach of their private information is common. Pew trust reported, 13% of American individuals have created their social media accounts hacked by an unauthorized person. Such hacking usually end up in using stolen information and forced shares that send followers to malware, among other things. Usually platforms of social media, which store and collect abundant personal information with limited government oversight, act as pleasing targets for bad users seeking to use that information to execute crime and fraud.

The concerns for privacy on social media have soared high in recent years. The growing concerns for privacy have paved way for a strict regulations. Additionally, these concerns made companies responsible for the security of the personal data under more scrutiny. Incidents concerning data breaches have agitated many users and prompted them to reconsider their personal relationships to social media and about the security of their personal data. Moreover, it has been noted that attack or issue against any online social site usually spread rapidly than other kinds of online attacks the reason being the trust that exist between the users of these network. Very common attacks to OSNs have been reviewed which also includes malware attacks, identity theft, sybil attacks and phishing. In order to counter these attacks proper measures are taken to maintain any sort of privacy and integrity concern and proper check and balance on the availability of information given by the users in their online profiles. Moreover, networking sites usually take everything into consideration, users are bound to a set of rule and they have a serious role in protecting their own information. However, users are also held responsible for any sort of content they share by ignoring the scenario that malicious users may access the content and initiate objectionable activities against them [4].

Definitions of the Terms

Social media social networking sites (SNS)

The definition of "what exactly Social Media and Social Networking Sites are" can't be restricted to any single definition. It is more of a description that how social media works by underlying the communication among individuals in which they are sharing, exchanging, creating, modifying their notions in virtual setups or groups: " Social Media is group of applications on internet that's created on ideological basis of Web 2.0, which allow the formation and exchange of user created Content" [5].

Carr and Hayes (2015) defined social media as "(...) Internet-based channels that allow users to opportunistically interact and selectively self-present, either in realtime or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others" (p. 50). They further pointed out that users' interaction will increasingly be influenced by social media affordances.

In describing SNS, Boyd and Ellison (2007) talks about the term "network" instead of using "networking" as according to them the later term signify relationship initiation, normally among strangers: … services that are web based that permit individuals to (1) make a profile either public or semi-public within a restrictive system, (2) list those users with whom they have a connection, and (3) check and traverse their list of connections and those created by others in the system. It's obvious that the nature and classification of these connection may differ according to the sites they use."

Kaplan and Haenlein (2010) in more similar yet restrictive manner describe social networking sites as: "… platforms or applications that allow users to connect by forming a profile based on personal information, inviting colleagues and friends to have access to these particular profiles, and sending and receiving messages and e-mails between them." This restrictive nature of Kaplan and Haenlein's definitions can be verified on the basis that they (a) restrict the bonds/connections to colleagues and friends; and (b) restrict SNS processes to e-mailing, profile access and messaging, therefore ignoring the sharing of information and other content.

Highlighting the processes of SNS, Richter and Koch (2008) describe them as ".. System of applications that offer users functionalities for managing identity (1) (i.e. the portrayal of the own person for instance in the form of a profile) and allow to stay

in touch (2) with other using it (and consequently the supervision of own contacts). De Valck et al. (2009) used the term "social networking sites" to explain other types of social media for instance wikis and content communities. Others consider using the term "online social networks" in a restrictive manner to only include those individuals who have common interest: "Online social networks are groups of those individuals who are partially or totally connected on the internet and share common interest (For instance, Facebook and MySpace)" [6].

Privacy

Privacy has been defined as the selective control of information sharing, where control is key. For social media, however, an individual user's informational control has become more difficult. A more comprehensive and prag-matic view was offered by Alan Westin as "... the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others". The psychological concept, as well as studies of everyday meanings of privacy, emphasize privacy as control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access [7].

In view of Beye(2010) the word privacy has many subtly different meanings, ranging from personal privacy (which includes seclusion and bodily privacy) to information privacy, each withtheir own definition. Privacy on the Web in general revolves mostly around Information Privacy, as defined below in the IITF wording that Kang uses:

Information Privacy is "an individual's claim to control the terms under which personal information-information identifiable to the individual-is acquired, disclosed or used." Recently, Barrett-Maitland and Lynch (2020) defined privacy as the right to be free from any kind of surveillance, to be left alone, or undesired disclosure of the personal information or data by any corporation, government, or individual.

Right to privacy

Although issues concerning privacy have become the hot topic lately as a problem of policy in the public discussion, interest in investigating concept of privacy while policy making and by the public is an old phenomenon. Interest in contemplating, defining and privacy protection can be drew back to the ground breaking work "The Right to Privacy" by the Boston law partners Samuel Warren and Louis Brandeis" which was published in 1890 by the Harvard Law Review. They advocated for the right to privacy, the paper published by them shaped and contributed in the development of treatment, the legal protection of privacy and recognition in the west. Today, sveryone has the right to the protection of the law against any interference or attacks". Many jurisdictions, including SouthKorea,15 Spain,16 Switzerland,1 Thailand, United States (US), and United Kingdom (UK) have recognised a right to privacy. It may be stated generally that privacy embraces four aspects, namely, information, bodily, communication, and territorial privacy.

A researcher in legal issues, William Prosser contended that the cases of privacy can be categorized into 4 interrelated "torts," that are [8].

Intrusion: it refers to infringement (physical or something else) on ones' freedoms/isolation in a quite hostile way.

Privacy facts: it refers to providing irrelevant or unnecessary information, regarding someone's public or private life.

False light: it refers to providing incorrect information or making "highly offensive" remarks about someone else.

Appropriation: it refers to stealing a person's identity (name, pictures) with an intention to gain advantage without the consent of that individual.

Privacy threats on social media

The advancement of Information Technology has hastened the ability to disseminate information across the globe. In particular, the recent trends in 'Social Networking' have led to a spark in personally sensitive information being published on the World Wide Web. While such socially active websites are creative tools for expressing one's personality it also entails serious privacy concerns. Thus, Social Networking websites could be termed a double edged sword.

A social engineering hack happened in the March of 2012, in which the hackers made a fake account on Facebook using the name of NATO's Supreme Allied Commander Europe (SACEUR)NATO's with the motive to intrigue his social circle and professional partners to reach him and then delude them to uncover secret data utilizing the methods of social engineering. After the profile was accounted for to Facebook, it was brought down and an examination started to catch the culprits. An attack like this is called reverse/anti engineering attack. This incident highlighted the loops in privacy framework of Facebook and similar networks. Reverse attack and some other major privacy threats are discussed below [9].

Social engineering and reverse social engineering attacks

A reverse engineering outbreak (attack) is another danger to OSNs in which the vindictive hackers tricks the media consumer into reaching him utilizing various kinds of strategies. As the user is the one who starts the contact, a more significant level of trust developed between the user and the hacker. After this association is set up with the target, the starts his noxious activities, for example, spamming and phishing.

Data scraping

It includes following individuals' life on the web and collecting personal information and discussions from online platforms, recruitment sites and social media. Normally, research organizations are the gatherers, and offer the gathered information to different organizations. These organizations ultimately utilize this data to structure the advertisement lobbies for their items. While one may contend that individuals are intentionally sharing personal data via online media and in this manner, it's free for everybody's utilization; information harvesters don't seek the consent of the owner. This raises a moral protection issue associated with OSNs [10].

Facebook Apps Leaking Personal Data

It has been highlighted numerous times that specific Facebook applications are spilling data about the users' identity, to marketing and advertisement firms without taking the users in confidence.

Online social tracking

All of us hit the "Like", "Tweet", "+1", and numerous other buttons to stay in touch with our social circle. These social interactions become a key source of data for online tracking sites. They operate using cookies-little records/documents saved in a PC that assist in tracking the client across various online networks-that social sites place in programs when you make a profile or sign in, and together they help the online sites in recognizing a particular individual on any site that uses these cookies. This implies that your inclinations and online shopping activities can be effectively followed and your web protection can be inconsiderately attacked [11].

- **Identity theft:** Access to fundamental data comprising the personality of the user (i.e., name, family name, date and place of birth, pictures) makes the way for such risks. This access makes it easy to steal anyone's online identity. This danger has been perceived and has prompted an adjustment in enactment in different parts of the world.

- **Pedophilia and sexual crimes**: It has been revealed that sexual predators target young people who are active on every type of social media network. Locations can often be traced by social media so these predators can track these youngsters by contacting them through social media by using fake account and fake identities. Teenagers are eager to make connections and friends on social networks, hence the are not too careful talking to strangers which increases the risk of falling a prey to these predators.

Advertising harassment/spam: According to Sandberg, the chief operating officer, Facebook earned an estimate of 4 billion US dollar by advertising in 2011. Other than Facebook, many other companies also display advertisements on various websites for promotional purposes. However, these advertisements also target specific Twitter introduced a concept called "sponsored tweet", which allows the advertisers to gain detailed information of profiles of users. This concept enables them find out about users more and then gain customers to increase their revenue. Spam is a real problem which not only affects the users of the website but also the creators are as much affected by it. Facebook was attacked with a pornographic spam campaign in fall 2011, due to which pornographic content was displayed in users' news feeds.

This implies that the modern times has brought many technological reforms like internet in our lives. However, it has changed the concept of privacy completely. Everybody can be able to track others through online location no matter where they are. It has created convenience as well as dangers to privacy to individuals. Understanding these dangers can solve these privacy issues.

Methodology

There are several methods that could be done to contemplate or grasp the concept of social media and its impact. The major portion of this research will be written on the basis of information taken from secondary qualitative sources such as reports, books, websites, press articles and analyses based on political researches, therefore using a qualitative methodology. A thorough examination will be carried out on the impacts and privacy concerns of social media.

Rationale

The online world today is so interwoven that users are continuously connected to one another and a lot of data is generated by every passing second. In these circumstances, it is important to investigate that to whom your data is accessible?, how much of your data is accessible? and what measures can be taken to protect this data online? [12]. Today, the technological providers like mobile applications, game creators and social media can access a huge amount of data that can be used to extract insights. As the website is according to the requirements of users, it increases the profit of the companies by gaining more user. It is no denying to the fact that social networks have become an integral part of our lives, it has led to Privacy Paradox, which means that even with great dangers this internet poses, individuals still share their data with it without a second thought.

The popularity of SNS continues to expand. The Pew Research Center in 2015 stated that about 90% of adults in America aged 18-29 use social sites as compared to 12% back in 2005, total increase of about 750%. 89% of Europeans in 2013 age ranging between 16 and 24 used social networks. These connection or usage can render users vulnerable in numerous ways. If personal data is accessed by wrong people, the consequences can be dire. The European Commission in 2012 asked for improving European Union (EU) data protection rules according to which residents should regain their control over their private data. Nowadays, mobile devices have become an integral part of our daily life. These have proven to be an advantageous scientific invention that fillspersonal and business needs in a very efficient manner. In this era, the availability of internet services has significantly increased because of the rich variety of social media platforms and essential applications provided by mobile device manufacturers [13]. At the same time, numerous internet security issues and data privacy threats are challenging both manufacturers and users. Therefore, social media platforms are an ideal target for various security issues and data privacy threats in a mobile ecosystem. This study will help understand and extract the online privacy concerns of the users (from the published literature) to get a better idea of domains, questions, and issues around which to anchor the intended objectives of the study. This will be achieved by performing an in-depth literature review.

Aim and Objectives

The research aim of this thesis is to explore the use and impact of social media on everyday life choices along with exploring the associated privacy paradox. To achieve this aim, this study focuses on active users' interactions with social media and how

this interaction impacts different domains of life. Moreover, it attempts to highlight the awareness of users regarding the privacy breach. Following the identification of the research aim, the following objectives of this study have been formulated:

Research objectives

1. To explore social media use and impact on everyday life choices.

2. To reveal the consequences of social media usage within the context of privacy.

3. To understand the level of awareness in public regarding the privacy breach.

4. To propose a model that will act as a framework for understanding use and impact of social media in third world countries like Pakistan.

5. To provide a deeper understanding of social media potential implications for political, academic, business, and marketing purposes.

Research questions

To achieve the objectives, the following research questions have been formulated:

1. How is social media use influencing the daily life choices?

2. How is social media breaching the privacy paradox?

3. What is the impact of social media prevalence on third world countries?

4. How social media impact active users' political view, consumer behaviour, academic and occupational life?

Legislative landscape

Many critics have attempted studies to learn deeply about the privacy dangers and their effects on the society. These studies raise awareness about practices and methods which should be adopted to protect one's privacy online. Privacy risks arise when individuals share their data online to strangers without knowing the people who view their information. This is because people do not take the privacy concerns in consideration.

Awareness regarding privacy policies and breach: Besides the privacy threats the social media poses, it is good platform for users all over the world to connect and communicate. However, with the increase in OSN users, more and more amount of data is available for social relations. The malicious users and hackers take advantage of loads of personal data available online. They target OSNs and attacks them using the data shared by the users. Therefore, the OSN users are at high risk of privacy breach on internet. Also OSN can become a source for criminals and hackers to perform cyber crimes such as spamming and stealing users' data through viruses and phishing which may result in releasing data of individuals and someone may use this data illegally. The main reason why criminals take advantage of OSN users is that they are not mindful of the value of their data and how it can be used against them. Therefore, they don't make attempts to secure their data against the attacks to cyber criminals. So the attackers smartly trick users into releasing their data and then use it to destroy the users reputation. This implies the significance of public's awareness regarding privacy breach and concerns.

Govani and Pashley (2005) tell about how much students are well aware about how to deal with privacy issues and the Facebook privacy policy that it provides to it's users. According to the study, most of the students are well aware of the security issues and privacy threats but however, they still feel comfortable sharing their data online. This can be attributed to the fact that they are unaware of the extent to which their personal data is vulnerable. Although, the students know how to protect their data and how to hide it from potential fraudulent users, still they don't make efforts in doing so. Tow et al. (2008) in his study also furthers the idea that either users are not aware of the risks online or they believe that the risks are not strong enough to affect them greatly. He states that another reason can be that the users perceive the online world to be safe and incapable of stealing their information without their consent.

Therefore, it is important for users to know that who can access the data you post on internet and on social media platforms. Ther term of personal identifiable information or personally identifying information (PII) is considered significant when discussing online and internet privacy threats and risks. It is the information about any individual that can be used to personally identify, make contact or know his/her location. It is important to understand this concept in the world where it has become so easy to extract information about anyone. If someone accesses the authorized information without consent, it may cause financial losses to the user. Apart from this the SNS security protocol is important to protect one's identity and reputation. And sometimes, the security breaches and loss of information can cause damages that are not fixable. Losing face among friends, revealing secret information, making social blunders, or simply giving a wrong impression. By facing these threats one may not be able to cope with the damage and even face the people around them. All in all, these threats can have very serious long term effects on individual's life. These problems are not taken seriously and are not explicitly discussed but awareness about them can solve many issues and make the life of individuals much easy.

Almost every website takes specific measures to protect the privacy of individuals and keep their users' data safe from beaches. Every platform should enable tools to ensure user friendly environment and keep a close eye on the privacy of individuals. It is important to keep privacy as prime priority so that users are encouraged to use the website with no fear of their data leaking out without their consent. Many social media platforms and SNS are criticized based on their settings that allows visibility of users accounts to a large number of audiences and there is no way to limit it by their own consent. Users data and information is available to everyone on these platforms and not just to their trusted people if they don't bother to change their privacy settings. Gross and Acquisti (2005) also raise the point that the interface of such platforms also make people reluctant to change their setting to protect their data. The privacy tools are of no use if the users doesn't make use of it. The study reveals that only a small number of users change their privacy setting,

exposing their data to everyone on that platform and there is no way to track who can access this information. Cranor et al. (2006) shows that even if the social media networks make an effort to make their interface easy and accessible, very small number of people change their settings on any of the software they use. The reason behind this can be that people don't like to waste their time or they are not so much aware of technology. It can also be due to the fear that they may mess up the setting and cause damage to their accounts. However, the privacy breaches cannot be solely attributed to users' negligence since the policy frameworks of SNS also have some major loopholes.

Major loopholes in privacy

Walking a fine line between effective marketing and privacy intrusion: Social media networks including Facebook and Twitter are changing and adapting consistently. But it is difficult to decide for them to protect their users' privacy over advertisement benefits especially when there isn't a financial incentive in place. So in order to target specific customers, companies gather information and attempt at privacy intrusions.

The privacy loophools location-based services: In today's fast growing world, individuals are more clinged to their smartphones than bother using computers for browsing internet. Due to this, social media platforms make use of location based services which increases the risk of privacy breaches and poses a threat to security of users. As smartphones mostly detect location automatically, social media platforms utilize most of this data continuously. Since not much check and balance is kept on social media services, they take great advantage of this fact. Absence of privacy laws makes it difficult for individuals to track every privacy breach. There are numerous cases in which stalkers and hackers steal your personal information because of location sharing by the social media accounts. Moreover, this might also be the reason for burglary and theft when you are away from home. Thus, these concerns highlight that strict legislative policies are requisite to ensure the privacy of users.

Legal and regulatory landscape

From the legislative perspective, security is principally ensured by universal and constitutional human rights, and by more explicit rules for protection of data. The European Union has been driving the improvement of the law for data protection. Be that as it may, as for new sort of administrations, for example, SNSs, the laws actually neglect to cover them sufficiently. The law for data protection is intended to protect people against malevolent crooks and overactive organizations, yet it scarcely specifies social connections between individuals.

In general, the European law restricts the processing of private data. For example, there has to be an acceptable purpose to process personal data and it is not allowed to use the data against that purpose. However, if the person gives consent, then almost any processing is allowed. In an SNS, people upload their private data into the site themselves. Therefore, arguably, the processing of that data is in accordance with their consent-as long as they have understood what kind of processing and usage of the data can take place. Thus, it is central what the end-user knows and understands about the privacy policy of an SNS and the principles according to which the data is processed. Just by publishing information, the end-user has probably not given consent to such processing that was unknown to him or her.

The Constitution of the Islamic Republic of Pakistan enshrines the right to privacy as a fundamental right. Article 14(1) of the Constitution confirms that "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable." As a fundamental constitutional right, the right to privacy is meant to take precedence over any other inconsistent provisions of domestic law. Article 8 of the Constitution provides that "[a]ny law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred [under the Constitution], shall, to the extent of such inconsistency, be void." Article 8 (5), furthermore, states that "[t]he rights conferred by this Chapter shall not be suspended except as expressly provided by the Constitution." Yet Pakistan's constitution also includes a wide-ranging exception to the primacy of fundamental rights.

Communication surveillance

On February 28, 2019, the Ministry of Information Technology and Telecommunication formed a Committee headed by the chairman of the PTA that will undertake a "broad-based consultation with relevant segments of civil society and technology companies about these rules and complete the process within two months." However, civil society organizations have said in a statement that as long as the rules are still approved by the Federal Cabinet and have not been withdrawn, the consultative process is "merely token to deflect criticism and not a genuine exercise to seek input." On March 3, 2020, Dawn newspaper asked the chairman of the PTA to clarify the current legal status of the rules. The chairman responded that "[t]he rules are expected to be improved/amended suitably at the end of consultation process. Implementation of [existing] rules has been suspended."

Right to privacy

In 2016, the National Assembly enacted the Prevention of Electronic Crimes Act ("PECA") to provide a comprehensive legal framework to define various kinds of electronic crimes, mechanisms for investigation, prosecution and adjudication in relation to electronic crimes.

Offences and punishments

Unauthorized access to information or data with dishonest intention shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

Literature Review

Knowledge is power. We all recognize this saying but few understand the empowering role social media has played. Through social media, anyone online is empowered by an unrestricted flow of information to add to their knowledge bank. In today's world, it is undeniable that social media plays an important role in impacting our culture, our economy and our overall view of the world. Social media is a new forum that brings people to exchange idea, connect with, relate to, and mobilize for a cause,

seek advice, and offer guidance. It has removed communication barriers and created decentralized communication channel and open the door for all to have a voice and participate in a democratic fashion including people in repressive countries. Although it has brought about many benefits, allowing us to easily connect with friends and family around the globe, allowing us to break down international borders and cultural barriers, social media has come at a price. It also has a negative impact on our lives because the combination of isolation and global reach has eroded our culture.

Social media is robbing us of trust and comfort we once placed in one another, replacing the human fellowship, physical and emotional support we once drew from each other with virtual connection. Now a days people, instead of giving time to family or friends, have started spending time on browsing and surfing internet. It is observed that due to this excessive use and investing plenty of time on internet emotional bonds are diminishing from families that was built because of daily social interactions and contact. It is reported to have a negative impact on individuals and on society.

A recent study by SANGWAAN (2019) highlighted that individuals can conveniently share data or impart through different long range social networking channels such as Facebook, Instagram and Twitter, among others. It tends to be embraced by somebody to get positive outcomes in all domains of life. Social interaction permits the people to exchange creative thoughts and make new learning. Sharing information gives a simple and a compelling manner by which one can share information and access the data.

As the innovation and technology is growing, interpersonal interaction and social mingling has transformed into an everyday practice for each individual or group, and they rely on it completely for their life choices including political views. In comparison to other media, social media's influence in political campaigns has increased tremendously. Social networks play an increasingly important role in electoral politics — first in the ultimately unsuccessful candidacy of Howard Dean in 2003, and then in the election of the first African-American president in 2008. It is reported by The New York Times that "The Donald J. Trump elections is probably the starkest demonstration all around the planet that social media networks are aiding on basic level to rewire the society". Since social media provides a platform for freely communicating with each other, it is creating astonishingly influential social communities within marginalized groups.

Political utilization of new media around the world, web-based media has become a platform for political commitment and, political conversations. It is quite a significant tool that has proved to have capacity to impact political opinions and even the behavior of casting a vote. Truly, political groups, have the option to control the data about themselves through deliberately placed press declarations and campaigns.

As people in general get influenced by peer pressure, in real world, it also impacts the academic world. Students appear to be more exposed to peer pressure at social sites. Within third world developing as well as developed nations students are getting more dependent on online media and its applications for multiple reasons. These reasons can prompt change in social and individual way of life both academically and otherwise. Students are one of the main clients of the virtual world and interpersonal networks. The abuse of informal social sites has both negative and positive scholastic, social, and well-being ramifications for the students. Decreased academic progress is one of the main results of social media usage for students.

Web-based media advances corporates' business, affiliations and brands which impact companions, by creating news, to create good relations and again make groups. One can comprehend the client requirement and advance the business everywhere in the world. It gives rich client encounters through checking and you can pick up key data about your rivals. In business, web-based media isn't thoroughly risk free, as negative comments can prompt a relationship with frustration and disappointment. An error made via online media is difficult to amend, which is the reason negative client audits are unsafe.

The outgrowth of social media means it's uncommon to discover an association that doesn't get to its clients through social platforms. Organizations see the significance of utilizing web-based media to associate with clients and construct revenue. Organizations have acknowledged they can utilize web-based media to create insights, invigorate request, and make focused on item contributions. Colossal information is moved and safe in seconds across the world to obscure servers. This influences the human and the general public overall additionally on another level: The Internet security, or online well-being. Strangely, in spite of the fact that the utilization of social interaction and sharing has become the exceptional standard of business, a few organizations, in the wake of encountering some negative impacts of online media, have chosen to contradict some common norms and eliminate the social sharing catches from their sites. In our current reality where the information stream is controlled by outer servers, information robbery and information assurance are the new trending words.

As the quantity of Internet clients and trade of User Generated Content expands every day around the world, Internet security is a developing concern for kids, grown-ups, associations and even nations. This could even prompt identity theft on a nearby or worldwide level. Occasions like Safer Internet Day should assist with bringing issues to light on the individual level. Increasingly more web destinations are made by governments or offices to make residents mindful about these new dangers of the individual character and free of individual information.

O'Keeffe and Clarke-Pearson (2011), also postulated that online media affected negatively more than positive side. It involves access to improper content without considering privacy and its policies. Moreover they said that after the involvement of web-based media, the ratio of online badgering, harassment, and cyberbullying has increased during their research and presented "signaling theory". As per the study hypothesis, an individual while attempting to make himself/herself famous on social media adds numerous unknown people in his/her friend list, and this is the way an individual trades off their own privacy and trust.

The privacy paradox explains people's readiness to reveal

personal data on these social sites despite voicing privacy concerns. Young and Quan-Hasse, (2013) in their research employed the distinction between social and institutional privacy to comprehend this phenomenon. They inquired about the tactic and strategies that undergraduate students have established and what exactly is the motivation behind using such tactics. They used a mixed method approach that included 21 detailed interviews and 77 surveys. The result of this study proposed that, in addition to the usage of default privacy setting, pupils have used many tactics to properly address their privacy concerns. The strategies or tactics are used to protect themselves against any threat and comprise of excluding information of contact, by using the option of limited profile, removing photos and un-tagging and restricting friendship requests from unfamiliar persons. These strategies of privacy are made to manage the Facebook profile, which we discuss functions as a front stage. This management of profile enables users to use Facebook with the need to increase privacy. Therefore the users reveal information, because they have already played their part by using these strategies to guard against the potential threats.

As per the "privacy paradox", although individuals assert that they take care of the privacy concerns but at the same time they share a lot of personal data through online media platforms. A study by Hargittai and Marwick (2016) uncovered that individuals in young adulthood do apprehend and worry about the potential dangers linked with providing personal information on the web, to a certain extent, and employ probably some security measures on social platforms. They believe that once an individual has shared information is on social media, it is eventually out of his/her control to completely secure it. They emphasize that this can be attributed to the obscure acts of establishments, the innovative affordances of online media, and the idea of networked privacy, which asserts that people exist in social settings where others can and do breach their privacy.

Usage of social media in third world countries: Pakistani perspective

With regards to the fame of SNS non-industrial nations also are at the cutting edge. In Pakistan web-based media is getting differentiation with every passing day. Thirty million individuals in Pakistan have been accounted for to be online consistently and the number is developing rapidly. Similarly, there are 120 million flexible endorsers in Pakistan that make it the fifth greatest cell phone grandstand in Asia. Face book is currently the most comprehensively used web-based media webpage in Pakistan with 9,000,000 customers in the country. It has been found that Facebook has more than 1,000,000 allies every month and 44 thousand new customers joining the site reliably. Pakistan's Facebook crowd has been accounted for to be 70% male, 30% female as of April 2013. Facebook has transformed into one of the key channels of correspondence between off-shore Pakistanis living in the Gulf States, European countries and the US and their families back home.

Pakistan's sizeable populace creates an immense amount of communication traffic. Approximately 73.36% of Pakistanis have a cell phone membership, as indicated by the Pakistan Telecommunications Authority. An estimated 22.2% of the populace utilizes the internet. Fifty operational internet facilitators and six mobile administrators serve this interest. Online media platforms are generally used in Pakistan. The informal organization Facebook supposedly had approximately 32 million Pakistani users in 2018. Twitter is assessed to have 3.1 million users. Pakistan additionally has a quickly developing publishing content to a blog network. Blogspot.com is positioned among the top five visited websites in Pakistanis, while the best 20 websites involve Facebook, YouTube, Daily-Motion, Blogger.com, Wordpress.com, Pinterest and Twitter.

Scholarship on the utilization of SNS is immense. Examination on SNS offers extensive record of its relationship with numerous viewpoints including brutality among youth and issues related with badgering coming about because of over the top utilization of online media. The part of online media in making activism has been investigated in different settings, the association of web-based media with social capital has been discussed, and the relationship of web-based media with character development has been examined. Past exploration has additionally featured the difficulties and openings identified with SNS across the world.

Since admittance to web gives worldwide availability to customers, it has offered new vistas of business worldwide for Pakistani youth. Youth residing in distant territories of Pakistan avail the overall opportunities and prospects. Pakistani youth successfully utilized and profited by new media to react the noxious missions against Islam. A few years back, when an outsider transferred a critical post about Holy Prophet Muhammad (P.B.U.H), the young lot used online media and enrolled their dissent around the world. These online exercises inspired and upheld the offline strikes and fights, which constrained the Pakistani government to eliminate and boycott such substance at the Internet. New media is additionally useful regarding the women empowerment. Actually, Pakistan is a male centric culture and the conventional media mirrors a component of sex predisposition in its content. Presently endeavors are being made to move Pakistani youth through online media to speak loudly against sex based brutality. In this way, new media is considered imperative to counter the negative effect of traditional media content.

In Pakistan, customary media is frequently reprimanded for being untrustworthy, working with popularized approach, and overlooking the editorial code of morals and ethics. Youth have engaged with useless and some of the time dangerous activities, which are projecting harmful impacts on society and its individuals. Albeit, new media has given the young lot different platforms to communicate their thoughts and opinions, however it is also considered as the lone source to deliver their dissatisfaction by talking against the things they disdain. While talking about any issue, the emotions, sensitivities and regards of others are totally dismissed. Political bodies are especially the core victims of that disappointment and bashing. For the sake of political communication and online political investment, shameless and injurious language against political bodies is embraced. Besides, posting unsophisticated content and deceptively photoshopped pictures of lawmakers has gotten a typical propensity among online networks.

Very recently, political utilization of new media was very less in Pakistan and political parties started using it in general elections of 2008, the country's political groups utilized their official sites and furthermore YouTube somewhat to extend their manifestos and other data. Anyway a short time later, political utilization of new media quickly turned out to be very successive.

In 2013 results after elections, practically all conspicuous political groups used new media to impact youngsters. Indeed, even now, the winning party and the Opposition with the assistance of new media engender their political perspectives. Likewise, youth are a lot of dynamic and active in digital world to safeguard their number one pioneers and leaders and react to the purposeful publicity against them. In Pakistan, web-based media has been utilized viably for spurring and assembling the youth. Especially during the hours of floods 2010, the adolescent gave combative updates through web-based media about relief efforts, restoration and about the requirements of victims.

Trust is a major concern that develops citizens' willingness to use social media as a technology platform for e-government services. However, despite its importance, there is lack of prior investigation about the factors that can generate citizens' trust to use such services, particularly in a developing country like Pakistan. The findings show a significant relationship of trust with citizens intention to use government social media services. Information quality, structural assurances, perceived security, perceived privacy and perceived ease of use are identified as antecedents of trust. The proposed model of this study explains 56.4% of the variance in trust. These findings can assist government organizations and policy makers in making decisions to increase citizens participation by facilitating their trust on social media-based services of e-government.

Moreover, Internet users in Pakistan have identified harassment and data privacy issues as their most pressing concerns online, according to a new study released by Media Matters for Democracy (MMfD) on Tuesday, July 30th, 2019. The study, titled "The Internet as we see it: Gendered perceptions from Pakistan", also found that men and women users agreed on the benefits of the web, such as connectivity and access to information, but differed in their reactions to harassment and restrictions on expression online. The MMfD study revealed an overwhelming majority of research participants understood the importance of data privacy and surveillance. Speaking about the findings, Amel Ghani, a program manager of MMfD and the co-author of the study, said, "Many believe that awareness and understanding of these issues in the general users in Pakistan is somewhat low, but it was really interesting to see a rather deep understanding of these issues in Pakistani user base" "Study Finds 'Online Harassment, 2019.

Theoretical framework

In only few decades, online media have changed the life of numerous individuals and accordingly pulled in much attention, from industry, yet additionally the scholarly community and academia. To understand the phenomenon, analysts have embraced theories, utilized literature and its constructs, and proposed theoretical frameworks.

Dependency theory: Dependency theory has been proposed by Ball-Rockeach and DeFleur in 1976. The theory postulates that the more an individual is dependent on a certain medium to have his or her needs fulfilled, the more important the medium will be to that individual for other activities. It posits that people gain information about all types of topics through media. They have to depend on media. Dependency relations with media developed among individuals through three ways. First, our understanding about world is formed by information which is delivered by media resources. Self-understanding enables one to understand information aboutoneself; as a result makes them able to interpret their behaviors, as well as to compare themselves with others. Second, orientation, either in terms of action or interactionmakes us dependent on media. Finally, media is considered as important source forprovision of opportunities. Since its introduction, this media dependency theory (MDT) has been applied to examine the relationships between individuals and various types of media, including newspapers, radio, magazines and television, to explain how various mediahave different cognitive, affective and behavioral effects on individuals' activities2 6 using the media. Thus, this theory best explains the excessive usage and impact of social media platforms.

Communication privacy management theory (CPM): Communication privacy management theory (CPM) provides a road map that explains a system to understand the communicative aspects of how people make judgments about managing their private information with other people. CPM theory is evidence-based and applied in focus. This means that the core aspects of this theoretical map have been tested to verify that the ideas ring true to the way people conduct their lives where managing private information is concerned. In today's world there is much discussion surrounding how people think about privacy within interpersonal relationships, families, healthcare, business, and especially interpersonal interactions in online social media. Privacy concerns permeate almost every aspect of our interactions including social media platforms. The goal of the CPM theory and research conducted using this theory is a better grasp of how choices are made and how to make them more beneficial for all types of interpersonal relationships.

Communication privacy management theory is centrally focused on how people define and subsequently communicate about their private information. Because the emphasis is on the communicative and social-behavioral aspects of privacy management, the understanding that is derived using a CPM framework is comprehensive and accounts for other people with whom individuals interact. In this regard, CPM theory takes the broadest view of interpersonal interactions.

There are four foundational aspects that guide an understanding about the way privacy management works. First, CPM assumes that regulating privacy access or protection is best explained as dialectical; that is, people need to be both social and autonomous simultaneously. Second, CPM offers several proven aspects about the nature of privacy regulation. That is, people believe they rightfully own their private information, even after they tell others or grant access to others. Third, CPM proposes that the best way to understand the management of ownership

and control over information is through the use of "privacy rules."Fourth, CPM uses the concept of a privacy boundary metaphor to more easily illustrate how people mark information as private. These boundaries can be described as "thick" when people are less likely to reveal information or "thin" when there is a higher possibility of people disclosing or allowing access.

Cognitive dissonance theory: In order to understand the relationship between variables of the study cognitive dissonance theory was taken under consideration. The terminologies dissonance and consonance alludes to relationships between pairs of elements. and these elements relate to what has been termed as thinking, to what one knows about oneself, to particular actions, and also about his environment. There is a possibility of three types of relationships between mental components, which include irrelevant relations (two cognitions tell nothing about one another and are irrelevant), dissonance (two cognitive elements do not match for some reason) and the third one, consonance (in which two cognitions are applicable and match each other). At the point when an individual stands up to new occasions or data, conflicting with his or her current thought process, for example, logical inconsistency, social mores and so forth, a condition of dissonance arises. Subsequently, the event of conflict may prompt mental distress, and therefore, people are constrained to attempt to decrease or reduce this instability (dissonance) and accomplish a state of stability (consonance). The premise of this theory is that individuals do not tolerate abnormalities or variability quite.

There are three different ways to reduce the caused dissonance. These are to change the behavioral element of cognition (changing behaviors), to change the environmental element of cognition (changing environment) or to add a new element of cognition in the existing pool (reconciling). Moreover, individuals deliberately avoid the information that can cause an increase in dissonance and try to seek information that is consistent with the existing cognitive elements. When an individual is no longer able to avoid the contradictory information he or she, starts using psychological processes to reduce the amount of dissonance. One of the processes is to reduce the amount of importance given to a particular element. According to the existing literature there are two ways that can be incorporated, either to use trivialization in which one has to minimizes or downgrades the importance given to dissonance or to use bolstering in which one puts more significance to the information that is consistent with the existing mental thoughts.

In our study, this theory helps to explain that how privacy threats on social media can influence one's decision about how much information he/she will share. When a person has a positive perception regarding data protection, there exists a strong consensus among their actions and their positive perception about privacy, hence the consistency among new information coming from outer world and the previously existing information gives rise to consonance. The individual end up accepting this new information as it is and adds it to the already existing pool of information which means that he or she will continue to share personal information on social media platforms. For instance, the user hears about strict government policies regarding privacy, it will futher strengthen his/her behavior of trusting the platform. However, when there is lack of consensus among existing belief and new set of information, state of dissonance arises, which leads to negative emotionality and discomfort. Which also indicates that these negative emotions can be linked to a precautionary measures to avoid the privacy breach., This implies that in case of dissonance, the user will either stop sharing personal information on social media platforms or will take precautionary measures like changing pivacy settings to ensure that the personal data is secure (in both the cases, changing the behaviour in order to reduce dissonance).

Terms of Use and Privacy Policies

"Privacy era is over". This is not some hacker's statement because of the hijacking of accounts but of the Mark Zuckerberg, the pioneer and executive chief of Facebook. k. And, though it prompted a public outcry, it also shows that how small importance social networking sites give to privacy of user. Hence, in spite of the fact that the Facebook states of utilization try regarding and ensuring the data of site individuals, a provision further indicates: "We do all that we can to make Facebook a protected help, yet can't ensure its supreme security. To do this, we need your assistance, which incorporates the accompanying commitment."A series of recommendations then follows.

So, usage of social networking is not the slightest bit fit for ensuring the well-being of Internet clients and are deliberately written so that will deter clients from browsing them appropriately. Websites essentially have no interest in clients finding certain conditions that give them full power over all the data distributed. Along these lines, in 2009, Facebook was guaranteeing lifetime responsibility for client data even after clients withdrew from the site. The site was then compelled to surrender this discreetly presented clause, confronted with the authentic objection incited by this choice. Unfortunately, privacy protection solutions offered by anyexisting OSN applications are revealed to be unsatisfactory no matter their robustness. Decentralized OSNs attempt to remedy to this problem by avoiding the adoption of any omniscient entity that can directly manage and misusethe user data and propose an infrastructure for user datamanagement and storage that is distributed. Such solutions still present some weaknesses in terms of privacy. Hence, due to the questionable behavior of administrators of the websites, every consumer should be educated about current enactment and afterward act capably to keep themselves protected. Following are some pecautionary measures that users should employ to reduce the vulnerability of their data.

Precautionary measures

Vigilance or cautiousness keeps on initiating the security and, consequently, the privacy of the data. It tends to be separated into a couple of strategies that are straightforward however could have a significant effect:

- **Choice of "friends" and contacts**: Users should be cautious in their selection of companions on these networking sites. It is normal practice to acknowledge contact from friend of friends, who are every now and again complete outsiders. This

can prompt one's private life being presented to conceivably destructive people.

- **Restricting private content from friends and family**: Social networking sites are progressively permitting their clients to design limitations on access to their data. It is, in this way, critical to utilize these limitations and to guarantee that they are appropriately arranged, given that our data is publicly at default.

- Careful choice of information to be broadcast: The key to the protection of privacy is in fact what information one broadcasts. Name, surname, date of birth, place of birth, photos, videos, comments and opinions should be carefully screened prior to being posted. Keep in mind that information posted on a network may one day be used against its author.

- Awareness: Every sector of the population should be made aware of the need to protect themselves against the risk that the use of social networks may entail. In the business world, this awareness must form part of the IT security program.

The role of OSN users

As clarified in past segments, clients of OSNs manage different kinds of privacy and security hazards. In this segment, we offer straightforward rules that can help OSN clients to upgrade security and privacy and ensure themselves against various sorts of assaults:

- Users should not share an excess of individual data in OSNs. Sharing superfluous private data inside an enormous network can furnish noxious clients to assemble or induce individual data about OSN clients, putting their privacy and security in danger.

- Users should not face the challenge of allowing friend request from obscure individuals, since such demands are probably going to come from vindictive clients.

- Going through the Terms of Use and Privacy Policies of the online social networking sites is prescribed to clients before enrollment.

- Since the default protection settings of OSNs are insufficient, clients are encouraged to adjust their settings in the start of joining an OSN with the goal that the data they share in their profile isn't noticeable to unknown individuals. For example, 'friends only' is particularly the most ideal choice among accessible degrees of protection settings and allows only friends to access the data partook in users profile.

- Installing Internet security programming is prescribed to ensure users personal data while surfing through OSNs. Another recommendation is to eliminate superfluous outsider applications that can conceivably accumulate individual data about the clients.

- OSN clients should be mindful about location based options given by social networking sites since they can uncover user locations and follow any advancement. Likewise, it is a decent practice that user don't share their contact, similar to email address, timetables, and schedules with others, which may permit vindictive users to follow them.

- Since kids are more prone to PC violations, their parents should screen their online activities. They should likewise instruct their kids about the characteristic threats of digital wrongdoings and show them the essential guidelines to finish while riding the Internet all in all and OSNs specifically.

- Users should report any issue they may have regarding their privacy and security, similar to spam, cyberbullying, or identity fraud. They ought to consider reaching the OSN supplier and local authorization offices or counseling proficient lawyers in the event that they think that they are the survivors of digital cyber bullying or crime. In outline, users should know about the way that once their own data is revealed on the web, there is no assurance that this data can be erased, since it might have been gathered via web engines or duplicated by different clients.

Discussion and Conclusion

Discussion

Social media is significantly modifying the way people talk and form relationships. Now Social Media is deemed as most used if not very effective medium for the distribution of information to numerous audiences. Social media has phenomenal power it even has the ability to downturn the governments (e.g., Moldova), by organizing protests and political campaigns, getting aid from humanitarian groups, forming groups to delay the ordaining of any bill and making users millionaires and billionaires.

Online social interactions and networking offer new open doors for connection and correspondence. The online climate is a simple and modest approach to keep up previously existing connections and present oneself to other people. Nonetheless, the expanding number of activities in online administrations additionally gives an ascent to protection concerns and dangers. Our examination shows, that the clients of social media apps appear to uncover a lot of data about themselves to a lot of both strong and frail associations, and sometimes here and there to individuals absolutely aliens to them. As in most comparable examinations, our subjects are generally youthful grown-ups and students. The outcomes show that they don't have critical protection concerns, yet claim to be genuinely mindful of security hazards. By and large, the privacy issues are seen to be more modest on Facebook than on the Internet all in all. One purpose behind this can be the way that "the Internet" is something huge and obscure, while Facebook is seen to be a more reasonable "social site". It is likely, that an extraordinary number of individuals, who don't utilize social media interactions, do so precisely due to security concerns.

Discussion of privacy and social network sites has tended to focus on the potential threat posed by either outside access, such as reidentifying profile pictures, demographic data, or unique interests from other SNS. Other outside threats may originate in the general use of unsecured login connections used by SNS allowing easy access for third parties, such as hackers, identity thieves, and government. However, there are further privacy issues within the SNS and the network of contacts, even if private information is willingly disclosed by a site user. These include the open discussion of personal information among contacts,

the posting and tagging of photographs that identify other users, disclosure of demographic data, and posting personal information on profile pages that implicates other users.

As mentioned above, privacy strategies appear to be significant. That isn't simply because they educate the users about the handling regarding private information, yet in addition they mostly characterize consent that the social media users have provided, when they transferred their private information into the administration. Thus, an intriguing inquiry for future exploration is the reason the users don't peruse privacy strategies of SNS's. Just like different researches have appeared, security and privacy policies and the terms of utilization simply don't stand out enough to be noticed by the users. There may be a few explanations behind this: it is seen to require an excess of exertion, they are hard to comprehend, or the clients trust the authorities so much that they believe they don't need to understand or red any policies. All things considered, as our research shows, in any event, perusing the privacy policies doesn't appear to build awareness about intentions of service providers. Most of the users are-or guarantee to be-mindful of security policies on SNSs and they have likewise utilized them. In any case, default settings can appear to be befuddling and some specific activities, for example, joining another network, may change settings without clients acknowledging it.

Besides, there are as yet numerous users whose profiles are exceptionally obvious to all the individuals from a specific organization and networks, which may incorporate a huge number of outsiders. Consequently, it stays a fascinating inquiry to which handling of private information the user has intentionally given their assents. In this paper, we have evaluated prior studies on privacy issues identified with informal social networking and websites, and introduced the consequences of our observational investigation among users of a specific SNS, Facebook. As the entire online climate and social networks specifically are genuinely new wonders, number of issues are not completely perceived by the users, who may even seem to act unreasonably. Security is a mind boggling construct and, in that capacity, hard to comprehend. In like manner, there are various elements that influence privacy patterns. Subsequently, more examination into security mindfulness and related conduct on social networking sites is obviously called for.

Conclusion

Social networks are an incredible method to communicate and share with other people. They help clients lift the boundaries of existence and speak with the entire world. Nonetheless, there have been other sides related with the demonstrated risks of user privacy infringement. It is concluded that there is significant tilt toward privacy concerns of social networks. Another concern arose about institutional privacy and no techniques were set up to shield against dangers from the utilization of personal information by organizations. This is applicable for strategy conversations, since it proposes that the assortment, accumulation, and usage of individual information for focused commercial have become an acknowledged accepted practice.

These dangers are even more of a threat now thanks to the increasingly widespread trend of registering on several sites using a single user account. In response to this situation, each Internet user must remain vigilant and governments must put more pressure on the operators of these sites in order to safeguard the security of Internet users.

Online social networks have increased disclosure of personal information by making more information available online. Despite all the proactive security monitoring technologies that are used by different online social networks nowadays, cyber attackers still find ways to accomplish malicious activities, like attacking computer systems, engaging in phishing activities and identity theft, cyber bullying, etc. Additionally, attacks against online social networks usually spread faster than other types of online attacks because of the trust existing among the users of the network. In this chapter, we have reviewed the most common attacks to OSNs, including identity theft, phishing, malware attacks, and sybil attacks. We have also discussed some countermeasures that can be used against these attacks in order to maintain privacy, integrity, and availability of data that is being shared by the users in their online profiles. However, taking everything into consideration, users have a critical role in protecting their own information by adhering to a set of security guidelines. Indeed, users themselves are responsible for any content that they share in their profiles, ignoring the fact that malicious users may find a way to access such content and initiate undesirable activities against them.

Social Media is widely used and boon and bane at the same time. It facilitates global communication in seconds, connects deserted areas with the civilisation, plays an important role in e-commerce and above all in the participation and democratisation process. But the list of disadvantages and threats is also long. It may be concluded that social media in Pakistan has been used as a modern tool for dissemination of personal and collective opinions. It is believed that positive use of social media may educate Pakistani youth and develop their knowledge, information and skills in academic terms. It can be used for socio-political awareness, enhance language proficiency and scholarly debates. The element of connectivity does help to develop inter-cultural relationships in cyber community. However, the misuse of new media technologies has become a big problem, imparting harmful effects on society and youth in particular. It is suggested that without restricting the digital rights and freedom of expression, efforts should be made to restrict the negative use of new media technologies.

References

1 Abass IAM (2018) Social engineering threat and defense: a literature survey. J Infor Security *9:* 257.

2 Acquisti A, Gross R (2006) Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy enha techn 4258: 36-58.

3 Ahmad T (2021) Pakistan: Federal Government Issues Controversial Rules On Social Media Content | Global Legal Monitor. Locgov Np 2020: 10.

4 Ali R (2016) Social media and youth in Pakistan: Implications on family relations. Global Med J *14*:

5 Ali Z, Jan M, Iqbal A (2013) Social media implication on politics of Pakistan. Measuring the impact of Facebook. Internat Asian res j 1: 13-21.

6 Alimoradi Z, Lin CY, Imani V, Griffiths MD, Pakpour AH, et al. (2019) Social media addiction and sexual dysfunction among Iranian women: The mediating role of intimacy and social support. J behav addict 8: 318-325.

7 Allen AL (1988) Uneasy access: Privacy for women in a free society. Rowman & Littlefield.

8 Amedie J (2015) The impact of social media on society.

9 Anderson KB, Durbin E, Salinger MA (2008) Identity theft. J Eco Perspec 22: 171-192.

10 Aral S, Dellarocas C, Godes D (2013) Introduction to the special issue-social media and business transformation: a framework for research. Infor Sys Res 24: 3-13.

11 Argyle, M. and Furnham, A., 1982. The ecology of relationships: Choice of situations as a function of relationship. British J Soc Psychol 21: 259-262.

12 Khan EA (2018) The Prevention of Electronic Crimes Act 2016: An Analysis. LUMS LJ 5: 117.

13 Assaad, W. and Gómez, J.M., 2011. Social network in marketing (social media marketing) opportunities and risks. Intern J Manag Public Sec Inform Communic Technol 2: 13.