



# INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES



## Privacy Paradox in Facebook: An Online Social Networking Site

Farhan Mirza, Muhammad Zeeshan Ashraf, Sarfraz Ashraf

To Link this Article: <http://dx.doi.org/10.6007/IJARBSS/v11-i4/8831>

DOI:10.6007/IJARBSS/v11-i4/8831

**Received:** 01 February 2021, **Revised:** 07 March 2021, **Accepted:** 25 March 2021

**Published Online:** 10 April 2021

**In-Text Citation:** (Mirza et al., 2021)

**To Cite this Article:** Mirza, F., Ashraf, M. Z., & Ashraf, S. (2021). Privacy Paradox in Facebook: An Online Social Networking Site. *International Journal of Academic Research in Business and Social Sciences*, 11(4), 1-19.

**Copyright:** © 2021 The Author(s)

Published by Human Resource Management Academic Research Society ([www.hrmars.com](http://www.hrmars.com))

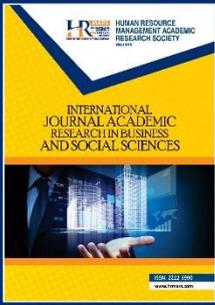
This article is published under the Creative Commons Attribution (CC BY 4.0) license. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this license may be seen at: <http://creativecommons.org/licenses/by/4.0/legalcode>

**Vol. 11, No. 4, 2021, Pg. 1 - 19**

<http://hrmars.com/index.php/pages/detail/IJARBSS>

JOURNAL HOMEPAGE

Full Terms & Conditions of access and use can be found at  
<http://hrmars.com/index.php/pages/detail/publication-ethics>



# INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES



## Privacy Paradox in Facebook: An Online Social Networking Site

<sup>1</sup>Farhan Mirza, <sup>2</sup>Muhammad Zeeshan Ashraf, <sup>3</sup>Sarfrax Ashraf

<sup>1</sup>HND Department, The Millennium Universal College, Queensberry Campus, Gujranwala,

<sup>2</sup>Department of Management Science, SZABIST Islamabad, <sup>3</sup>MBA (3.5) University of Sargodha, Gujranwala

Email: sarfrax.ashraf@gmail.com

### Abstract

Privacy in using the internet is a debating topic in the field of social networking. In this regard, the objective of the study is to determine the factors associated with the disclosure of the information by the user on social networking sites. However, this study has found seven key factors associated with disclosure of information which include the realization of privacy, understanding of privacy statements, trust in friends and family, data distortion, data transferring, data profiling, and control on information shared over Facebook. This study has gathered data by using a non-probability convenient sampling procedure and collected data from 215 Facebook users by using a survey strategy. The survey questionnaire has been formulated by using measurement scales from existing literature. The findings of the study have reported that realization of privacy and control on shared information are insignificantly impacted on the disclosure behavior of the user. However, data distortion, data transferring, and data profiling adversely and significantly impacted the disclosure behavior of the users. In contrast, understanding of privacy statements and trust in friends and family positively and significantly influenced the disclosure behavior of the users. Based on such generalizable findings, this study has also provided significant implications along with future avenues of the research.

**Keywords:** Privacy Paradox, Social Networking, Facebook, Disclosure Behavior of Users.

### Introduction

A total of 500 million users is there, of social networking site named Facebook in this world and Asia this reach towards 8.2 billion internet users and among them almost 1 billion Facebook users (Brailovskaia et al., 2020). Social networking is a place where the user-generated data is being exchanged or one can say being shared. It can now imagine the data sharing of this huge population over social networking sites. The approximate statistics of Facebook each month of the data is as under;

- 3 billion photos uploads
- 5,00,000 active applications (Tobin et al., 2020)

Just in Asia, the average age of the Facebook user is range 18-24 years and Facebook is the 3<sup>rd</sup> highest search term on google.com in Pakistan. Pakistan has 5.8 million users of Facebook which ranked Pakistan as 25<sup>th</sup> placed country. The dominant age group in Pakistan is 18-24 years, which is almost more than half of the Facebook users in Pakistan. Tobin et al., (2020) has confirmed that on average, a Facebook user has:

- “130 friends in a profile,
- Sends 8 friend requests per month,
- Spends more than 55 minutes per day on Facebook,
- Clicks the Like button on 9 pieces of content each month,
- Writes 25 comments on Facebook content each month,
- Becomes a fan of 2 Pages each month,
- Invited to 3 events per month,
- Member of 12 groups and many more” (P. 259).

From such information provided above, one can imagine the data disclose on social networking sites like Facebook. So there comes the concern for user privacy when the bulk amount of data is being shared in an online community (Fuchs, 2012). The primary basis of this paper is to understand the factors due to which the privacy of the user is not much concerned while disclosing the online data. It is a challenge for the administrator of the social networking sites to provide its user more control and safeguards to protect privacy. Last researches show that only the identity and date of birth is enough to provide the identity thief a key for messing with someone and respondent are much happy to reveal all information (Sophos 2007). Prior literature showed that awareness among the people and education and understanding about the internet are the factors through which privacy concerns can be satisfied (Dinev & Hart 2005). Lack of understanding is still there to know about the fact that why still majority of the people deny to their privacy concern while sharing online from their perspectives and within their context. In this high age of technology world, people are part of many online communities like forums, blogs, and social networking sites. All of these online activities bring people together and people interact with each other so that they can share a different type of information, opinions, ideas exchange, and express feelings. This community includes a set of people who are connected by social relationships like friends, co-workers, or just for the sake of information exchange (Brown, 2020). Users in the online community are keeping sharing their ideas, thoughts, and daily activities. Such data could be used for some secondary purpose by many of the organizations and other sources. This data could be used in some criminal activities or some other uses. Users in the online community are unaware of such uses and willingly disclose their information (Iftikhar et al., 2017). Sometimes these data can be sold out to several organizations or can be used in some kind of business collaboration to achieve some specific goal. For example, Tumblr sold its user's information to Yahoo!. In some business collaborations, these data sets could be separated into a unique character of the segment to target them more accurately in their marketing mix strategies. Therefore, this paper is about to investigate the factors due to which users in the online community feel free to disclose their information.

In the last couple of years, there comes an enormous boost of online socialization and hence a lot of user-generated materials. Online social networks have become an important part of our daily routine life. Networking possibilities, obtaining social info and support as well as establishing and maintaining social connections are the reason to participate by the user (Malik et al., 2016). Online social networking sites are the places where users can express and feel their social pleasure and trigger curiosity as well as emotional and hedonic experiences

(Hart et al. 2008). Not only the participation rate in social network sites increases in the last couple of years but also the amount and type of information that a user in the online social community voluntarily discloses has been staggering. In contrast to the increasing fame of Facebook. Paine et al. (2006) stated that the privacy concerns of the people are diminishing 70% to 56%, which once was conducted by Hoadley et al., (2010) in the response to the same question. O'Brien and Torres (2012) investigate that although there someone can show their concerns about privacy while sharing their personal information on social network sites, but still busy in some context to the risky behavior. According to the survey conducted by the National Security Alliance (NCSA) in the United States, a total of 57% of the users of social network sites, among them 74% disclose their information like email, name, and a birthday date (Brandtzæg et al., 2010). Acquisti and Gross (2006) said that it is little or no relation between respondent's reported privacy concern and their disclosure behavior certain information. The same is the case with the Pakistani user. They ranked the privacy behavior much above the average ranking, but still busy in information discloses. This led the researcher towards the objective of this study that is to understand what are the factors behind that users have still engaged themselves in disclosure behavior in online social networking sites like Facebook in the Pakistani context. It's not the case that users are not aware of the risks associated but their concerns are not reflected in their actual behavior. This phenomenon is called the "privacy paradox" (e.g., Wilson et al., 2012) or "Privacy Dilemma" (Chalklen & Anderson, 2017). Some experts of IT said that "Social networking appears to provide a rich setting for criminal activities and other misdeeds" (Pandey & Gudipudi, 2019, P. 227). From the online social networks, it is evidence that millions of social network users, on the other hand, don't hesitate to share their thoughts, experiences, images, files or other kinds of stuff in such an environment that is largely barren of security standards and practices. Users are inclined to trust other community members with expertise, identity, mind matching and, personal information (Young & Quan-Haase, 2013). Users are also inclined to trust providers of social network sites to keep their information and photos private. From this, it appears that social networking takes place within a (largely pointless) framework of trust. The only use of social networking sites is practically not possible and unwanted. It needs to take initiative steps in the right direction, although given the willingness of users to share information. Before given the willingness of uses to share information, it needs to know the factors which lead users to engage them in risky online behavior. Many of the previous researches find out the scale for such kind of behaviors, there is little work on why people knowingly go for disclosure information which leads them towards risks. This leads the researcher towards the purpose of this study that is investigating the question that why the user doesn't consider their privacy while sharing in online social network sites like Facebook in the Pakistani context.

However, the objective of the study is to determine the factors associated with the disclosure of the information by the user on social networking sites.

## **Literature Review**

### **What is a Social Networking Site?**

To use a public or semi-public profile within a bounded system, individuals define the social networking sites, such as Web services so that they can borrow, view and the connection list and the list of computers within the other users with whom you share a connection with him by others, and Internet and interests so you can connect users through, and media and exchange activities (Kuss & Griffiths, 2017).

### **Online Social Networking Sites (OSN) Stakeholders Users**

Facebook (Facebook), Google, and others growing significantly every day millions of active users. Social network users, and companies, in particular, support individuals and service OSN, which is linked to an organization with profiles on the Internet (Akçayır, 2017). Able not only to create and manage relationships with their common interests such as development and recreation, as well as profiles management, social events based on the user or other technical issues OSN users. In this way, you can build a community in the online world of social relations and users with similar interests or the physical world. Social network users to download their contact list and contact details of a multimedia message and browse lists of content, and private and/or public, reviews, opinions, and recommendations (advanced user), you can also write a comment.

### **Social Network Operators**

For example, the user connected to primary care, for example, provides the server and access to various social networking sites and the plug and require replacing any user of enterprise data storage infrastructure. The program is attractive, an operator identification, and application programming interface (API) for use by third parties for the distribution of these additional services (Sohrabi & Karimi, 2018). Therefore, companies and other companies are expanding their services without a reboot of a social network, and you can count on the interface that is a platform for social networking via the Internet can be. The existing websites and social networking services create a growing collaboration and communication for individuals and the social environment in the web client (Ayaburi & Treku, 2020). Entrusted to the approval of a large amount of sensitive personal data on social networking and online social networks has led to an operator.

### **Third Parties**

The operators offer applications, services, and functions of the third person or organization other than a social network. They build and applications and services (such as games, music sharing, and personalized advertising) may depend on the API defined by the operator of a social network that can be deployed (Faelens et al., 2019). Attractive features, applications, and services are accessible to the user's information service are designed in a way that can be obtained (identification, contact, characteristics, such as research on the history of the navigation messages). Researchers are eager to study the similarities between advertising agencies and different types of third parties, the typical behavior of the user's behavior and the physical environment in the cyber world; In particular, the following scene ARS government agencies with an interest in Prevent a single domain and user profiles, and collect other detailed information on the activities of social unrest social networking and crime, the data collector (Faelens et al., 2019).

### **Data Collection and Usage**

In most cases, such OSN providers monetize all your data and financial services. The data can be divided into the actual (real) data acquisition and unconscious user. Of course, the difference will vary by the user. For non-native service, that is, a third-party service that is generated by the motor must be the same for the third-party user to access, such as certain information. In the final storage or redistribution, do not know what exactly to collect data (Stieglitz et al., 2018). Most users are unaware of the fact that the provider collects his actions, detailed information on the history, and the near surfing. This data (transparent to the user)

in / 1-button, the mechanism of server-side, shown cookies and collected this collection and then improved the operator and customization services, but also (for example, owners of the infrastructure and livestock the data used to pay for) to generate the resources revenue (Sehar et al., 2019). The data can be used, one for each user or group of users based on the use of data mining methods that personalize systematically. Data mining companies to new trends, market, or user needs at an early stage.

### **OSNs and mobile apps as CRM**

Online social networks and mobile applications bring new possibilities among customers, marketing, advertising, and open communication (Chang et al., 2017). They like it; you should be on the performance of a very important role in the management of customer relationships. User-selectable depending on the individual and OSN case is related to the benefits to the seller to rely on contacts with like-minded with their friends. Consumer decisions announced any ads for the product by a friend is likely to be the best individual circumstances.

### **Empirical Literature Review**

The origin of this paper is a condition which is frequently called the “privacy paradox”. It - refers to the fact that people used social networking sites sufficiently and disclose their data too willingly but still having some kind of fear in their minds and feel insecure sometimes and which are mostly justified some exaggerated (Zia et al., 2021). In other words, it can be observed coexistence of acceptance and fear as far as the use of social networking sites is concerned. This paradox may hinder the enormous potential of the Internet for users, businesses, and the economy, as users may be reluctant to use services that could benefit them significantly.

Activity in the online platform is being started with the creation and exposure of information and contents (Farsi et al., 2017; Tsay-Vogel et al., 2018). In online social networking sites like Facebook, many things engage a user busy and online which include picture sharing and uploading, status uploading, commenting on others' pictures & status, tagging friends, and many interesting links & pages. However, all of these are depending upon the user's online privacy concerns which can further affect the amount of data shared as well as the type of the data. (Lankton et al., 2017), which is, on the other hand, may have some kind of propositions of the social networking sites and their basic purpose of existing. In simpler words, one individual who has more privacy realization may disclose less information on social networking site. A user who is much concerned about the data sharing on online social networking sites may harm the personal unintentional disclosing behavior (Haimson et al., 2018), and physical threats (Osatuyi et al., 2018). They further found that understanding of privacy policy of the social networking site and control on information shared tools are the important factors. The general approach towards privacy is the vital role-playing practices. Now it is the challenge to the social networking site's administrators to effectively address such kind of user's privacy concerns so that privacy concerns can play a vital role in online disclosure behavior. In the last researches, authors find out that the relationship between privacy concerns and disclosure behavior may be settled through education about the understanding of privacy policy concerns and providing the users better information controls tools so that they can easily share their data (Haimson et al., 2018; Liu et al., 2017; Proudfoot et al., 2018). When administrators address such kinds of issues then the user can freely share their information online with many of the other users and also then engage themselves in community-enhancing behavior (Waterloo et al., 2018). Therefore, one can imagine the

strong relationship between the privacy concerns of the user and their online disclosure behavior.

Social networking nowadays is a part of our daily life. The majority of people use computers, smartphones, and tablets. Social network sites like Facebook topped with 1 billion users. It is a relatively new thing to publish personal information online. Many social network sites are enjoying their success, which is likely to continue. Facebook is also one of the most famous social networking sites. According to Millham and Atkin (2018), 89% of the user's names on Facebook are valid and through such a trend it can say that "Facebook is Google of People". Real name disclosure behavior is not just a problem since almost all of the data that is being shared in the online community are published regardless of the user's realization of the privacy issues (Farhan et al., 2020). Such actions are essentially the result of decreasing concerns within the online space as the millions of users of social networking sites like Facebook are at risk.

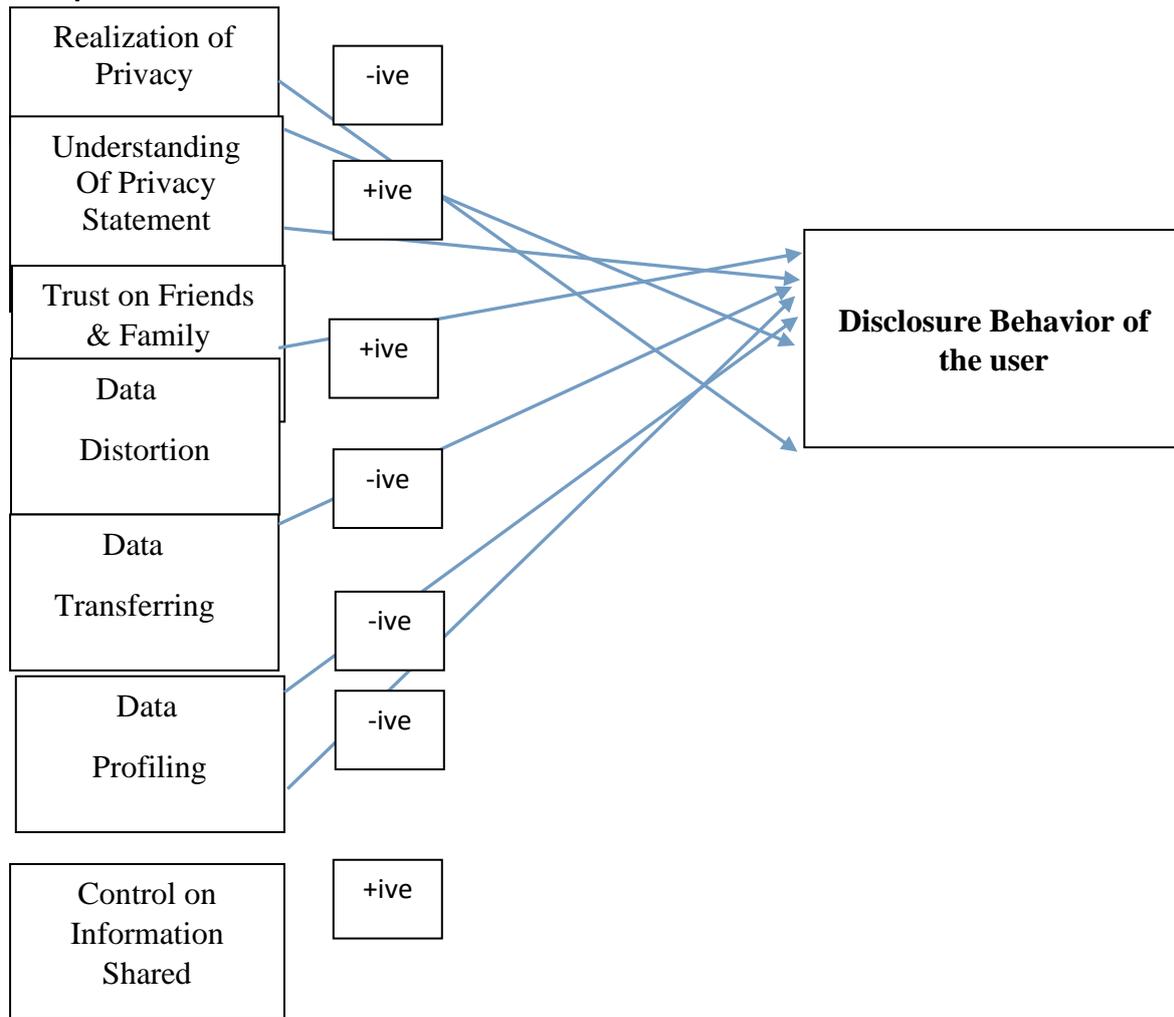
A social networking site's privacy policy is the statement that describes the usage of its user's data and also the protections that a user has. In short, this is the statement through which a user can inform about what will be going to happen with the data they share. According to Batenburg and Bartels (2017), they researched the privacy policy of social networking sites and find out 45 social networking sites, all have a privacy statement. It is the general norm in the consumer's mind that privacy policy is just a waste of time and difficult to read. Recent research studies find that there is a possibility that if a social networking site has its privacy statement then people tend to share more information on that site (Koohikamali et al., 2017; Liang et al., 2017; Spottswood & Hancock, 2017). In this study, the researcher mainly focuses on the understanding of the privacy policy. A variety of variables can influence the relationship between privacy understanding and disclosure behavior. According to Ashuri et al., (2018) network composition can exert influence on the relationship between privacy understanding and disclosure practices. Previous work identifies that privacy policy is time-consuming while reading the privacy policy is linked with less information disclosure in Facebook (Ashraf et al., 2018; Ashuri et al., 2018; Koohikamali et al., 2017). Yu et al., (2020) also find that there would be less disclosure if a social networking site has a privacy statement. Chen and Sharma (2015) highlight the role of self-similarity in a friendship connection of social networking sites like Facebook. In social networking sites like Facebook, a person generally accumulates many contacts, including the person you know as well as the contacts, work colleagues, and the people you met over the years. A user may have many unknown friends, which they don't know personally, and add them just because they are your friends of some of your friends or people with similar interests/group joined.

On a macro level, the social networks can be defined as the set of actors and set of ties that show a relationship or lack of relationship among the actors (Ashuri et al., 2018). Actors in a social network are individuals, organizations, or other social entities, and all of these are connected with the same kind of relationships like friendship, affiliation, financial exchange, or just simple information exchange. According to Chen and Sharma (2015), a social network is a collectivity of individuals among different kinds of information exchange with common norms and trustworthy behavior (Waterloo et al., 2018). In the last few years, many online social networking sites allow users to connect (Haimson et al., 2018). One feature of social networks is that to use not only connect too many new people and make connections but also the fact that user's friendship network is exposed and partially visible for other members (Ashuri et al., 2018). Online social networks like Facebook can attract many diverse audiences based on common interests or share racial, sexual, religious, or national-based identities (Park

et al., 2011). There are many social networking sites for many reasons, for example, Facebook is primarily friendship-oriented, Linked-In such as for the business purpose, and Match.com for romantic-oriented relationship initiations (Ashraf et al., 2018). The user of social network shares their information that infers self-disclosure as well as the active contribution that is the chief functional mechanism. If a user doesn't share anything, then networking can't be taking place. If jointly say a user starts with an individual user profile (Ashuri et al., 2018) and afterward, creation and use of existing and new relationships with other users become the vital reason of online social network (Liu et al., 2017). Therefore, trust in many other online users has to be there for the existence of social mechanisms. Online social networking sites like Facebook, allow their users to connect with known friends as well as provide anonymity. It facilitates the provision of false or misleading information or lacking or impeding verification mechanisms. In this situation of uncertainty, trust can assist as a central mechanism to reduce uncertainty and complexity of exchanges and relationships. Trust is the factor that could be seen as a mental "shortcut" that enables users to promptly absorb trust-related behaviors that are the provision of personal information.

In this context bounded regulation theories of privacy highlight the individual's knowledge about communication while sharing in online communities. As a person has many types of contacts added to their friend's list, there are many privacy levels as well. You can customize the privacy levels according to your own need or requirement, but it could be a very dangerous tool in the hand of the wrong person. Online social networks offer facilities and tools users can use to (re) connect, interact and connect with (hundreds of) other members of the network friends, acquaintances, colleagues, and other like-minded users (Ashraf et al., 2017). These tools are provided just to provide the user the control over the information that they share in the online community. The more the control on the information shared in online networking sites like Facebook, the more the user would disclose the information. Learning from their personal information disclosed may help them to differentiate about potential harmful activities from daily and regular activities that they are performing in the online community.

### Conceptual Framework



### Methodology

#### Methods and Procedures in Data Collection

This study is more concerned with the pragmatic investigation of the privacy paradox existence in online social networking sites. The factors which have been identified in the conceptual framework of this paper includes the realization of privacy, understanding of the privacy statement, trust in friends and family, data distortion, data transfer, data profiling, and control on information shared in online social networking sites as the independent variable while the information disclosure behavior of the Facebook user is the dependent variable. The respondents were asked to rate each item on the following 5-point Likert scale where “1 means strongly disagree, 2 means disagree, 3 means neutral, 4 means agree, and 5 means strongly agree”.

A quantitative research approach is being used in this paper as there is less amount of information available on the privacy paradox of social networking sites (Park et al., 2011). This is the best approach to use when a researcher dealing with the understanding of the complex social phenomenon (Malik et al., 2016). This type of study provides the best in-depth information about a typical type of phenomenon (Park et al., 2011) but the drawback of such kind of study is the lack of generalized findings. Although a quantitative study provides a baseline for the developing theories, although it doesn't explain the variance between variables (Fuller et al., 2016). Since the last many types of research provide a healthy insight

on the respective components of privacy paradox, this study is more focused on quantitative research

A sample size of 215 respondents was selected (out of 250) to fill the instrument. The respondents include the consumers, male & females, of different universities and organizations from Gujranwala, Rawalpindi, and Islamabad. The researcher has collected data through a non-probability sampling technique, i.e., convenient sampling has been applied.

### Measures

The instrument was developed to adapt as well as developed. For developing the questionnaire there is a further need for literature review regarding each factor/dimension. Help was sought from practitioners, academic experts, and previous studies. For the realization of privacy, 5 items were adapted from Dinev et al., (2006). Understanding of the privacy statement includes 4 items. Trust of Friends & Family consists of 4 items, Data distortion has 4 items, Data transferring has 3 items, Data profiling has 4 items, Control on information shared has 3 items, and dependent variable comprised of 9 items.

### Data Analysis and Findings

#### Reliability Analysis

To ensure the internal consistency of the instrument Cronbach alpha was computed. Realization of the privacy, understanding of the statement, the trust of friends & family, Data distortion, Data transfer, Data profiling, Control on information shared, and Disclosure in online social sites were checked. Cronbach Alpha for Realization of the privacy is 0.794, Understanding of the statement is 0.781, the trust of friends & family is 0.894, Data distortion has 0.752, Data transfer has 0.780, Data profiling has 0.786, Control on information shared has 0.742, Disclosure in online social sites is 0.880. The value of Cronbach alpha should be greater than 0.70 (Nunnally, 1978). These results enabled the study to proceed safely as all the dimensions were attractively greater than the critical value and, in some cases. Thus, it can state that measurement scales of the study possessed relevant internal consistency and able for further analysis.

Table 1: Reliability

Variable Name	Cronbach's Alpha	Items
Realization of the privacy	.794	5
Understanding of the privacy statement	.781	4
Trust on friends & family	.894	4
Data distortion	.752	4
Data transfer	.780	3
Data profiling	.786	4
Control on information shared	.742	3
Information disclosure behavior	.880	9

### Descriptive of the Demographic

Table 2 given below consists of demographics in percentage that how many of the respondents were male and how many were female, their age group, their profession, and the average time that an individual is spending daily on Facebook. The questionnaires which were collected back were 215 out of 250 (86%) shows that among 215 respondents 153 (71.2%) were 'Male' along with 61 (28.4%) were 'Female'. The age group as shown in table 2 represents the respondent ranging from 21-25 were 76 (35.3%), respondents whose ages were from 26-30 were 139 (64.7%). Table 2 given below also shows that participants had different professions. Table 2 below shows that 211 (98.1%) are students and 4 respondents were employed (1.9%) in the survey. Table 2 also represents the average daily time spends on Facebook by the respondent. 12 respondents (5.6%) spend less than 30 minutes, 124 respondents (57.7%) spend 30-60 minutes daily, 3 respondents (1.4%) spend 1-1.5 hours daily, 1 respondent (0.5%) spend 1.5-2 hours daily and 75 respondents (34.9%) are 24/7 online on their smartphone or any other gadgets.

Table 2: Demographic Information

Objects	Computation	Percentage
Gender		
Male	153	71.2
Female	62	28.4
Age group		
21-25 Years	76	35.3
26 to 30 years	139	64.7
Profession		
Student	211	98.1
Employee	04	1.9
Daily Time Spend		
<30 Minutes	12	5.60
20 to 60 Minutes	124	57.7
1 to 1.5 Hours	3	1.40
1.5 to 2 Hours	1	5.00
24/7 Hours	75	34.9

### Correlation

Correlation among the main variables of the study is shown in table 3 below. Table 3 below shows that there is a weak or no relationship between the realization of privacy and information disclosure behavior. The table given below shows that there is a significant positive relation between understanding of the privacy statement, trust in friends & family, and data distortion. It is shown in the below table that the relation between control on information shared, data transfer, and data profiling is weak.

Table 3: Correlation

Variables	1	2	3	4	5	6	7	8
ROP	1							
UOPS	.35*	1						
TOFF	.04**	.64*	1					
COIS	.08*	.32*	.39**	1				
DBU	.20**	.88*	.90*	.38**	1			
DD	.02*	.57*	.53*	.21*	.62*	1		
DT	.16*	.16**	.19**	.15**	.20**	.58**	1	
DP	.11**	.13*	.06*	.60*	.09*	.22*	.33**	1

### Regression Analysis

For the verification of all the hypotheses mentioned in the literature review, regression analysis was performed. More in regression analysis, all the demographics which are gender, age, qualification, and marital status were plotted as a control variable as they were being identified in ANOVA as a control variable.

*Hypothesis 1:* In the literature review it has been hypothesized that realization of privacy negatively affects information disclosure behavior as the same result has been found from the previous study conducted by different researchers, this study does not result in the same and was found that the more the individual realize about the privacy the more is the chance that he/she would disclose more information in social networking sites like Facebook as the value of  $\beta$  and its significance level from the table given below shows it ( $\beta = -.011^{**}$ ,  $p > 0.05$ ). So, from this result hypothesis 1 in which it has been hypothesized that realization of privacy negatively affects the information disclosure behavior is rejected.

*Hypothesis 2:* In a literature review, the hypothesis H2 in which it has been hypothesized that understanding of the privacy statement positively affects online information disclosure behavior, which is accepted, as the value of  $\beta$  and its significance level given in the table below shows it ( $\beta = .522$ ,  $p < 0.05$ ) and the result as according to the literature.

*Hypothesis 3:* More the hypothesis of trust on friends & family with information disclosure behavior (H3) is accepted which also means that Trust in Friends & Family will positively affect information disclosure behavior of the Facebook user, as shown in Table 4 given below, the value of  $\beta$  and its level of significance confirms it ( $\beta = .551^{**}$ ,  $p < 0.05$ ). The more they trust an individual has on the added friends & family members in their social networking group will result in more information disclosure behavior.

*Hypothesis 4:* Data distortion affects information disclosure behavior negatively, it was hypothesized (H4) in the literature review and it is accepted as shown in table 4 and the value of  $\beta$  and its level of significance given in the below table confirms the hypothesis ( $\beta = .061^{***}$ ,  $p < .05$ ).

*Hypothesis 5:* Hypothesis H5 is also accepted, in which it has been hypothesized in the literature review that the more the data transfer of the user's information which they shared in the online community, the less the information is disclosed by the user and it has been confirmed from the value of  $\beta$  and its significance level given in table 4 below ( $\beta = -.023^*$ ,  $p < 0.05$ ).

*Hypothesis 6:* Hypothesis H6 is also accepted which has been hypothesized in the literature review that data profiling of the user's shared information in online networking sites like Facebook will lead towards less information disclosure by the individuals and it is confirmed from the value of  $\beta$  and its significance level given in the table below ( $\beta = -.005^{***}$ ,  $p < 0.05$ ).

*Hypothesis 7:* The hypothesis H7 is also rejected which has been hypothesized in the literature review that the more the user in online social networking site like Facebook got the control, the more they will share their information and it is confirmed from the value of  $\beta$  and its significance level given in the table below ( $\beta = -.0150^{***}$ ,  $p > 0.05$ ).

Table 4: Regression Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig. P
	B	Std. Error			
(Constant)	.110	.032		3.407	.001
ROP	-.009	.004	-.011	-1.894	.060
UOPS	.493	.008	.522	64.580	.000
TOFF	.456	.006	.551	73.391	.000
COIS	.211	.005	-.015	-2.124	.203
DD	-.072	.009	.061	7.644	.000
DT	-.325	.007	-.023	-3.549	.000
DP	-.204	.005	-.005	-.759	.003

a. Dependent Variable: IDBM

### Summary of the Hypotheses

This study has formulated a total of seven hypotheses. The summary of the hypotheses based on empirical findings has been presented in the following table.

Table 5: Hypotheses Summary

Hypothesis	Summary
<b>H1:</b> Realization of privacy negatively affects information disclosure behavior of the Facebook user.	Rejected
<b>H2:</b> Understanding the privacy statement will lead to the less information disclosure behavior of the Facebook user.	Accepted
<b>H3:</b> Trust in Friends & Family will positively affect the information disclosure behavior of the Facebook user.	Accepted
<b>H4:</b> Data distortion of the Facebook user will lead towards less information disclosure behavior of the Facebook user.	Accepted
<b>H5:</b> Data transfer of Facebook users negatively affects the information disclosure behavior of the Facebook user.	Accepted
<b>H6:</b> Data profiling of Facebook users in the online community negatively affects the information disclosure behavior.	Accepted
<b>H7:</b> Control on information shared by the user on Facebook results in more information disclosure behavior of the user.	Rejected

### **Discussion and Conclusion**

The finding of this paper is corresponding with the last researches and it further enriches the theoretical understanding of information disclosure behavior. The very same thing was demonstrated by Dinev and Hart (2005), they determine the relationship exists between social awareness and privacy on social networking sites. Furthermore, it is quite undeniable that the suggestions from Lankton et al., (2017) that education is the essential point still holds. A user in the online social network must be reminded that they have control over what they are sharing in the online community.

This section summarizes the overall study and the consequences of the result achieved. All of the above-mentioned variables are extracting from the interviews from the respondent as well as from the literature. There are many things that a user has to say about the factors which they consider the most while sharing in the online community. Researcher finds out that the privacy realization, understanding of the privacy statement and trust in their friends and family members, data distortion, data transfer, data profiling, and control on information shared in the online social network, are the most important factors therefore, users feel free to share in the online social networking sites like Facebook. More than this, the user changes their settings from the default settings provided by the website developer and also customize them according to their own need. A user changes these settings and adds people who are more credible to them and their integrity is not questionable in any sense. By concluded at this stage, the researcher finds out that due to the trust of FNF users on Facebook, they share their information. The same thing was told to the researcher in the interviewing phase that they add only those users who are personally known to them or familiar with and their integrity is not questionable. More than this, respondents were also satisfied with the tools provided to them by the social networking developer. One can easily customize the settings according to one's privacy level and concerns in online social networking sites. In the correlation section, the same is the pattern as well as in the regression analysis section. Due to all this, Pakistani users feel safe in the online social community but this could be much dangerous if this would be in the wrong hand of the person.

Firstly, this study has confirmed that privacy realization is adversely linked with disclosure behavior of users, while such findings are not supported because it is insignificant. Secondly, understanding of privacy statements and trust in family and friends substantially influence disclosure behavior of users, while control of information is not a significant predictor of disclosure behavior. In contrast, data distortion, data transfer, and data profiling are adversely linked with disclosure behavior which is also supported by the statistical findings. In the same sense, prior research studies have confirmed that when a user has control over shared information and perceive that Facebook is offering constructive privacy statement, then users will demonstrate constructive behavior in using social media (Hasan et al., 2019). It implies that the findings of the study are aligned with existing literature and enable Facebook users to better understand organizational behavior toward their usage of Facebook.

### **Theoretical Implications of the Study**

This study contributes to the understanding that what are the reasons for Pakistani Facebook users to disclose their information on social networking sites like Facebook. At the start point, the researcher makes obvious the in-significant and no correlation between the realization of the privacy and understanding of the statement with the information disclosed by the user. Then researchers find out that trust of their friends and family while adding into the friend list and the privacy controls that a user has on Facebook are the reason to disclose a huge

amount of data on daily basis in the Pakistani social context. The important empirical findings will be helpful for the developers and designers of the social networking sites to better understand and provide the user more privacy controls (Hasan et al., 2019). According to the study, privacy is background and contingent information practice. By knowing the Pakistani users in their context, this study contributes to the growing body of work and to exploring privacy attitudes behavior on a macro level. As the number of Facebook users is increasing rapidly in Pakistan and it's the need of time to mitigate privacy concerns for the Pakistani users at the same time, are encouraged to share safely. This is the chief concern for the developers of Facebook as well. The importance of this study is mutually beneficial for the developers and many other advertisers as they have to address the privacy concerns and also the transparency needs of the users. Such explanation could inform operators of social network systems such as Facebook and contribute to the development of policies and procedures to more effectively educate users. These important empirical findings will provide insight for designers and maintainers of social media as they consider the implementation of privacy features.

### **Recommendations**

These recommendations apply to education, ethics, technology, legal issues, and research applications. Reduce the complexity and limit the number of application areas to ensure careful scientific evaluation. First of all, it is highly recommended that users should add only those users which are personally known to them at most priority. Secondly, never disclose their last name in online social networks. One can use the secondary e-mail address for socializing in the online community as if harassed by someone or developers for marketing and advertising purpose (Mirza et al., 2020). It would not bother them. Third, users can use the virtual private network (VPN) as it would be almost impossible for people with immoral intentions to get them in trouble.

### **Limitations and Future Roadmap of the Study**

As with many of the other studies, this paper also got some limitations. The very first is the data examined which is self-reported and it could be the source of potential error. Secondly, the divergent sample population, low response rate, and evidence of potential gender bias could limit the generalizability of the result of this study. Further, only the university students were selected as the unit of analysis which also limits the results of this paper. Different units of analysis in a different area of the country or world could lead to different outcomes. Furthermore, this paper only investigates one single social networking site like Facebook. There is a possibility that a contextual factor related to some specific social networking sites brings different results. Also, the data was cross-sectional which further leads towards the un-casual claims about the results.

Furthermore, due to limited time frame, budget, and some other reasons, the sample respondents were targeted to just 3 cities (Gujranwala, Rawalpindi & Islamabad). The other part of the country is not included in this study. The assumption may be valid to some extent but the perception of people outside the area might vary accordingly. Furthermore, larger sample size can be included in the study to get more generalized results.

## References

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*, 29(1), 36-58.
- Akçayır, G. (2017). Why do faculty members use or not use social networking sites for education? *Computers in Human Behavior*, 71, 378-385.
- Ashraf, S., Ilyas, R., Imtiaz, M., & Ahmad, S. (2018). Impact of service quality, corporate image and perceived value on brand loyalty with presence and absence of customer satisfaction: A study of four service sectors of Pakistan. *International Journal of Academic Research in Business and Social Sciences*, 8(2), 452-474.
- Ashraf, S., Ilyas, R., Imtiaz, M., & Tahir, H. M. (2017). Impact of CSR on customer loyalty: putting customer trust, customer identification, customer satisfaction and customer commitment into equation-a study on the banking sector of Pakistan. *International Journal of Multidisciplinary and Current Research*, 5(5), 1362-1372.
- Ashraf, S., Iftikhar, A., Yameen, A., & Younas, S. (2018). Empirical Relationship of Customer Brand Engagement with Satisfaction and Loyalty Through Online Brand Experience. *IUP Journal of Brand Management*, 15(3), 23-48.
- Ashuri, T., Dvir-Gvisman, S., & Halperin, R. (2018). Watching me watching you: How observational learning affects self-disclosure on social network sites? *Journal of Computer-Mediated Communication*, 23(1), 34-68.
- Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50, 171-181.
- Batenburg, A., & Bartels, J. (2017). Keeping up online appearances: How self-disclosure on Facebook affects perceived respect and likability in the professional context. *Computers in Human Behavior*, 74, 265-276.
- Brailovskaia, J., Ströse, F., Schillack, H., & Margraf, J. (2020). Less Facebook use—More well-being and a healthier lifestyle? An experimental intervention studies. *Computers in Human Behavior*, 108, 106-132.
- Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook “friends”? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human-Computer Interaction*, 26(11-12), 1006-1030.
- Brown, A. J. (2020). “Should I Stay or Should I Leave?”: Exploring (Dis) continued Facebook Use After the Cambridge Analytica Scandal. *Social Media+ Society*, 6(1), 2056-2069.
- Chalklen, C., & Anderson, H. (2017). Mothering on Facebook: Exploring the privacy/openness paradox. *Social Media+ Society*, 3(2), 1078-1091.
- Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior*, 69, 207-217.
- Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: the case of Facebook users. *European Journal of Information Systems*, 24(1), 93-106.
- Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management (JGIM)*, 14(4), 57-93.

- Faelens, L., Hoorelbeke, K., Fried, E., De Raedt, R., & Koster, E. H. (2019). Negative influences of Facebook use through the lens of network analysis. *Computers in Human Behavior, 96*, 13-22.
- Farci, M., Rossi, L., Boccia Artieri, G., & Giglietto, F. (2017). Networked intimacy. Intimacy and friendship among Italian Facebook users. *Information, Communication & Society, 20*(5), 784-801.
- Farhan, F. M., Waheed, N. A., & Younis, S. (2020). Impact of service quality and perceived value on the post-purchase intention with the moderating effect of switching cost. *Pakistan Journal of Multidisciplinary Research, 1*(1), 65-83.
- Fuchs, C. (2012). The political economy of privacy on Facebook. *Television & New Media, 13*(2), 139-159.
- Fuller, C. M., Simmering, M. J., Atinc, G., Atinc, Y., & Babin, B. J. (2016). Common methods variance detection in business research. *Journal of Business Research, 69*(8), 3192-3198.
- Haimson, O. L., Andalibi, N., De Choudhury, M., & Hayes, G. R. (2018). Relationship breakup disclosures and media ideologies on Facebook. *New Media & Society, 20*(5), 1931-1952.
- Hasan, A., Farhan, M., Khalid, Z., Komal, N., & Yaqoob, H. (2019). Impact of Stigma on Survivor's Productivity: Moderating Role of Perceived Organizational Support. *Int J Fam Busi Manag, 3*(1), 1-7.
- Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications, 9*(1), 50-60.
- Iftikhar, A., Azam, F., Ashraf, S., & Tahir, H. M. (2017). Exploring the Relationship Between Religiosity, Brand Trust and Green Purchase Intention as a Catalyst of Attitude. *Int. J. of Multidisciplinary and Current research, 5*, 1485-1493.
- Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior, 69*, 29-42.
- Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International journal of environmental research and public health, 14*(3), 311-329.
- Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior, 76*, 149-163.
- Liang, H., Shen, F., & Fu, K. W. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *new media & society, 19*(9), 1476-1497.
- Liu, Y., Rui, J. R., & Cui, X. (2017). Are people willing to share their political opinions on Facebook? Exploring roles of self-presentational concern in spiral of silence. *Computers in Human Behavior, 76*, 294-302.
- Malik, A., Hiekkänen, K., Dhir, A., & Nieminen, M. (2016). Impact of privacy, trust and user activity on intentions to share Facebook photos. *Journal of Information, Communication and Ethics in Society, 29*(1), 761-784.
- Millham, M. H., & Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society, 20*(1), 50-67.

- Mirza, F., Ashraf, S., & Jahangir, H. B. (2020). The Impact of Religiously Motivated Consumer Boycotts on Product Judgment, Brand Image and Loyalty. *International Journal of Academic Research in Business and Social Sciences*, 10(11), 384-402.
- Nunnally, J. C. (1978). *Psychometric theory* (2nd edit.) mcgraw-hill. Hillsdale, NJ, 416.
- O'Brien, D., & Torres, A. M. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 31(2), 63-77.
- Osatuyi, B., Passerini, K., Ravarini, A., & Grandhi, S. A. (2018). "Fool me once, shame on you... then, I learn." An examination of information disclosure in social networking sites. *Computers in human behavior*, 83, 73-86.
- Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65(6), 526-536.
- Pandey, N., & Gudipudi, B. (2019). Understanding 'what is privacy' for millennials on Facebook in India. *Journal of Data Protection & Privacy*, 2(3), 224-233.
- Park, N., Jin, B., & Jin, S. A. A. (2011). Effects of self-disclosure on relational intimacy in Facebook. *Computers in Human Behavior*, 27(5), 1974-1983.
- Proudfoot, J. G., Wilson, D., Valacich, J. S., & Byrd, M. D. (2018). Saving face on Facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, 37(1), 16-37.
- Sehar, R., Ashraf, S., & Azam, F. (2019). The influence of social media's marketing efforts on brand equity and consumer response. *IUP Journal of Marketing Management*, 18(2), 30-53.
- Sohrabi, M. K., & Karimi, F. (2018). A feature selection approach to detect spam in the Facebook social network. *Arabian Journal for Science and Engineering*, 43(2), 949-958.
- Sophos (2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves, [media release], Available from <http://www.sophos.com/pressoffice/news/articles/2007/08/Facebook.html>
- Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, 22(2), 55-70.
- Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics—Challenges in topic discovery, data collection, and data preparation. *International journal of information management*, 39, 156-168.
- Tobin, S. J., Chant, G., & Clay, R. (2020). Interpersonal goals as predictors of Facebook use, social capital, and envy. *Cyberpsychology, Behavior, and Social Networking*, 23(4), 257-263.
- Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *new media & society*, 20(1), 141-161.
- Waterloo, S. F., Baumgartner, S. E., Peter, J., & Valkenburg, P. M. (2018). Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *new media & society*, 20(5), 1813-1831.
- Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on psychological science*, 7(3), 203-220.
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479-500.

- Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 102-115.
- Zia, A., Younus, S., & Mirza, F. (2021). Investigating the Impact of Brand Image and Brand Loyalty on Brand Equity: The Mediating Role of Brand Awareness. *International Journal of Innovation, Creativity and Change*, 15(2), 1091-1106.