PRIVACY MANAGEMENT PRACTICES ON FACEBOOK"FACTORS AFFECTING DISCLOSURE OF PRIVATE INFORMATION AND USE OF PRIVACY SETTINGS"

Sherry Essam Hanna[*]
Under the Supervision of
Prof. Dr. Hebatallah El-Semary[*]

ABSTRACT

The purpose of this study was to investigate, through descriptive research, the current privacy management practices of Facebook users. Specifically, this study sought to explore factors that may help explain behaviors of disclosing private information on Facebook and using on-site privacy controls as well as providing understanding of each factor's contribution to explaining both behaviors. Factors tested in this study were drawn from the communication privacy management theory as well as online-privacy-related literature. 487 participants of active Facebook users were purposively chosen to answer an online questionnaire developed to collect the empirical data of this study. Bivariate correlations were first used to examine the relations between independent and dependent variables. Multiple Regression Modeling Analysis was then conducted to identify the factors leading to the aforementioned behaviors. Findings suggested the potential of Facebook use rate, motives, perceived control, awareness, trust in Facebook users, prior invasion, protective settings use, gender, and education as a framework to explain privacy management practices of Facebook users.

KEY WORDS: Online privacy, Communication privacy management theory, Disclosure, Facebook settings, Culture, Motives, Perceived benefits/risks, Control, Awareness, Concerns, Trust, and Prior invasion.

1. STUDY OVERVIEW AND THEORETICAL FRAMEWORK

1.1 Introduction

[*] Teaching Assistant at Radio & Television Department.Faculty of Mass Communication - Cairo University

[*] Professor at Radio and Television Department.Faculty of Mass Communication - Cairo University

Online social networking has become a mass adoption seeing that SNSs are now utilized by a large majority of internet users around the world. According to the annual global digital report, 42 million of internet users are active social media users in Egypt and there has been a 7.3% increase in the number of social media users by 2.9 million since April 2019, as of January 2020. Egyptian internet users spend an average of 2 hours and 57 minutes on social media each day to experience the advantages of social media and almost instant communication to potentially billions of other people. However, with advantages, there are often drawbacks, the most common of which are privacy breaches. Given that the subject of "Facebook and privacy" has lately drawn the attention of academic research due to the global popularity of Facebook as well as media attention to its privacy measures, it is the prime focus of this study. Online users are often concerned about how their shared private information and pictures are used and the degree of control they have over their dissemination. Notwithstanding the risks, individuals continue to choose to disclose more private information on Facebook and other SNSs. As a result, the current study was directed at the goal of explaining how Facebook users manage their information revelation and/or concealment decisions.

1.2 Statement of the Problem

Concerns about personal privacy on SNSs, like Facebook, have troubled internet users worldwide lately. Yet this does not keep individuals from frequently using it nor prevent them from willingly sharing private information and pictures about themselves and others. In light of this ongoing tension, this study was meant to focus on Facebook users' privacy management and consequent disclosure practices as well as how relevant factors might play a role in making decisions of information revelation/concealment through the use of Facebook privacy settings.

1.3 Objective of the Study

The main objective of this study was to shed the light on practices of privacy management among Facebook users through identifying factors that may help explain behaviors of voluntary disclosure of private information and usage of on-site privacy controls in a more holistic way.

1.4 Significance of the Study

Given the time frame of the latest Cambridge Analytica scandal, recent developments in Facebook after Mark Zuckerberg has pledged to secure the platform more, have heightened the need for studying users' disclosure behaviors and privacy management practices influenced by further concerns after the scandal. Furthermore, the scarcity of studies tackling the issue of privacy management in the Egyptian society calls for attention. In addition, we, researchers, have a social responsibility to educate online users about their digital footprints, and thereby helping them become privacy literate. Previous researchers may have examined this topic, but not with the depth of coverage of this study. Moreover, the study explores a variety of factors, some of which have been overlooked by previous researchers, which may help explain both behaviors and come up with a reliable model that should be able to elaborate the influencing factors of privacy management practices on SNSs.

1.5 Theoretical Framework

1.5.1 Communication Privacy Management Theory

The theory proposes five basic suppositions that underpin the rule management processes for privacy regulation. Supposition 1 states that when we reveal, we disclose private information. While some information about one's self is rather public, there is other information about one's self that is rather private or intimate and is disclosed under special circumstances. Supposition 2 states that private information is surrounded by boundaries either personal or collective. Boundaries may be permeable or impenetrable and are linked with other privacy boundaries. There are life span changes for a person's privacy boundaries. Supposition 3 states that one has the right to own and control private information and determine who is privileged to know about it and who is not. Supposition 4 states that the rule management system depends on three management processes that regulate the degree of revealing and concealing. The first is the privacy rule foundations process which represents how the rules develop and their properties.

The second process is that of boundary coordination reflecting how privacy is regulated through rules when people manage collective boundaries. Third, there is the process of boundary turbulence that takes place when coordination does not function in a synchronized way. Supposition 5 states that there is a dialectical tension between the needs of being both private through concealing and public through revealing (Petronio, 2002). All five theoretical suppositions are illustrated in Figure 1.1, page 3.

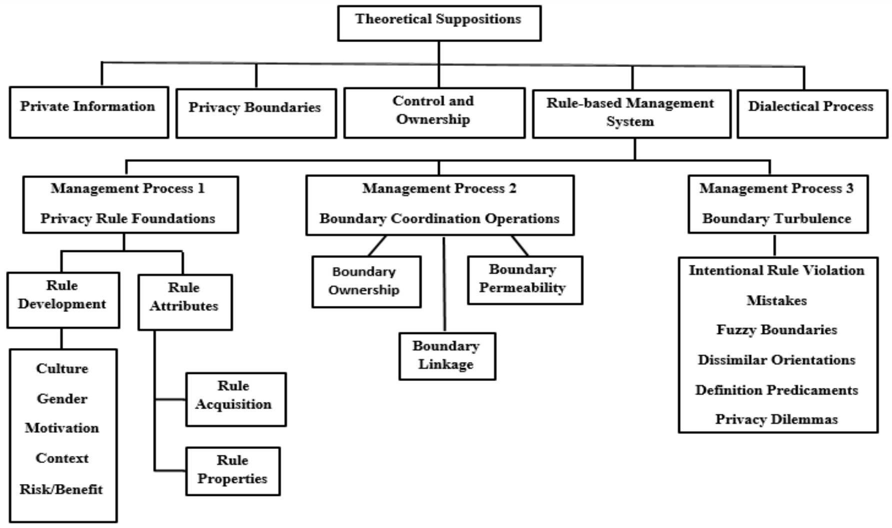

Fig. 1.1

Communication Privacy Management Theory Map[i]

1.5.2 Application of CPM Theory on Facebook

If a Facebook user keeps private information and does not share it on Facebook, the information remains within the personal boundary. On the contrary, if Facebook users divulge private information and share it with their friends and followers, the information then belongs to the collective boundary. Regulating the collective boundary involve regulating the site's privacy settings and disclosures. If Facebook users do not secure their Facebook account, thereby letting the general public and online prowlers have access to its contents, posts can pass on to the public realm and the collective boundary further broadens. Despite the fact that individuals usually end up giving up some control once private information is revealed, they associate any information they share to their own Facebook profile with a sense of ownership. Personal privacy rules are essential in the way one controls their Facebook content. For example, like every other culture, the Egyptian culture has values about disclosure that establish the basis for judging levels of privacy. Facebook serves as a unique interaction context and environment that guide users' decisions about what to share, how much to share, and with whom to share information. Women showed more concern for privacy management processes and protected information in collective boundaries more than did men (Child, 2007). Moreover, the more motivated one is, say to present oneself in a certain way, the more one weakens the borders of their boundaries. In like manner, when Facebook users perceive potential risks for disclosure of private information, they may tend to restrict access to their private information (Child & Westermann, 2013). For those on Facebook, a collective boundary is established with all who have been accepted as friends and anyone that has access to the profile content depending on the Facebook privacy settings instated by the user (Child et al., 2009).

Boundary ownership in Facebook resembles the privileges granted to the Facebook account owner, friends, and followers of revealed private information. Boundary permeability in Facebook features the amount of information that is able to go through the boundary after Facebook users' disclosure of private information to others. Boundary linkages in Facebook refer to the formation of collective boundaries through disclosing private information among other Facebook users (Cross & Shimonski, 2014). Rules for ownership, permeability, and linkages on Facebook can be coordinated in ways that either grant more public access or provide more protection of private information. Turbulence can occur if Facebook users come across private information uploaded on our personal accounts. Turbulence also takes place when we presume that only friends we know will access private information and pictures we post on Facebook (Child & Petronio, 2011). Another factor that can lead to turbulence can be when one reveals private information that belongs to another person or even a non-personal private photo on Facebook by mistake (Child et al., 2009). Such violations can make users adjust their disclosure practices or limit others' ability to be co-owners of parts of their Facebook profile content (Petronio, 2004). On Facebook, users can manage their privacy by not disclosing private information to that collective boundary. If they did, they can make use of the site's privacy-protection settings to reduce the possibility of boundary turbulence and privacy breaches.

1.6 Conceptual Framework

Based on CPM theory and insights of previous literature, Figure 1.2 in page 5 illustrates the proposed causal model suggesting that the independent variables of Facebook use rate, culture, motives for disclosure, perceived benefits/risks, perceived control over shared information, awareness, privacy concerns, trust whether in Facebook or other users, prior invasions and demographics are hypothesized to have an effect on the dependent variable of Facebook privacy-protection settings use that contributes in turn to disclosing private information on the site along with the other factors.

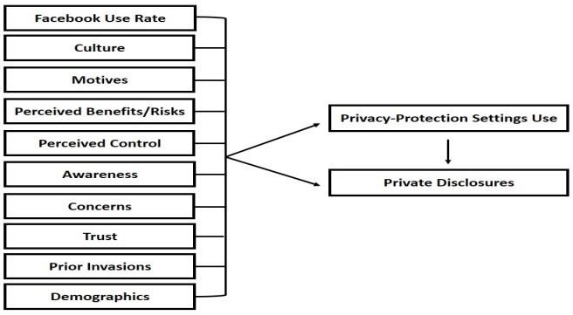

Fig. 1.2
Causal Conceptual Framework

1.6.1 Hypotheses

H1: Use of Facebook privacy-protection settings is predicted by a) Facebook use rate, b) individualism, c) collectivism, d) motives for private disclosures, e) perceived benefits, f) perceived risks, g) perceived control over shared information, h) awareness, i) privacy concerns, j) trust in Facebook, k) trust in Facebook users, l) prior invasion, m) gender, n) age, and o) educational level.

H2: Disclosure of private information on Facebook is predicted by a) Facebook use rate, b) individualism, c) collectivism, d) motives for private disclosures, e) perceived benefits, f) perceived risks, g) perceived control over shared information, h) awareness, i) privacy concerns, j) trust in Facebook, k) trust in Facebook users, l) prior invasions, m) use of Facebook privacy-protection settings, n) gender, o) age, and p) educational level.

1.7 Organization of the Study

The overall structure of the study takes the form of five chapters. Chapter 1 included an introductory background of the topic, statement of the problem, significance of the study, objectives of the study, theoretical and conceptual frameworks. Chapter 2 will present a review of the literature pertaining to online privacy and disclosure practices. Chapter 3 will describe the methodology used for this study. It includes selection of participants, data collection procedures and analysis. Chapter 4 will present the hypotheses test results. Lastly, chapter 5 will provide a discussion of the findings, limitations and recommendations for further research, and final conclusions.

2. REVIEW OF LITERATURE

2.1 Concept of Privacy

Westin (1970) defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (P. 7). In the same vein, Altman (1975) defines privacy as "selective control of access to the self or to one's group" (p. 18). Both authors refer to privacy as a "dynamic process of boundary management" (Westin 1970; Altman 1975). The strategies used for privacy management are related to a group of cultural preferences (Lewis et al., 2008; Papacharissi & Gibson, 2014). Middle Eastern cultures are considered to be powerful and consistent because they have a system of values, beliefs, and ideals that are well respected and honored by all members. According to several studies, individualism versus collectivism is considered one of the underlying pattern variables that are influenced by culture and influence human action (Hofstede & Bond, 1984; Petronio, 2000; 2002; Child et al., 2009; Petronio, 2013). Hofstede's findings indicate that Western countries tend toward strong individualism while tribalism is an important social factor in many Arab nations and African societies (Hofstede & Bond, 1984; Hofstede, 2005; 2006; Hofstede et al., 2010).

2.2 Online Social Networking

In Egypt, there are 42 million active social media users as of January 2020, resembling 41% of the total population. This is a 7.3% increase since April 2019. 63.5% of social media users in Egypt are males, and 36.5 % are females, with an average of 2 hours and 57 minutes spent using social media on a daily basis (We are social & Hootsuite, 2020). The biggest social network worldwide is Facebook which was launched in 2004 by Zuckerberg. According to the global digital report, Facebook comes second to Google as the most visited website in Egypt, based on monthly traffic, with an average of 13 minutes and 24 seconds per visit as of January 2020. Moreover, it is the leading social media platform in the country with 38 million users, resembling 91% of the total population of internet users in Egypt. This is a 2.7% increase since August 2019. SNSs users encounter many privacy risks. Some of the most common include cyber-stalking, cyberbullying, and social engineering (Cleary & Felici, 2014; Cross & Shimonski, 2014; Papacharissi & Gibson, 2014; Patchin, 2019).

2.3 Online Private Disclosures

Nowadays, users, especially males and teenagers, share personal information with large and potential unknown numbers of friends and strangers altogether (Tuunainen et al., 2009). Besides, many users befriend other users whom they would not consider friends in a non-cyber environment (Govani & Pashley, 2005; Gross et al., 2005; Blatterer, 2010; Aljohani et al., 2016). There are several different reasons for sharing information with people in SNSs, among which is the fear of missing out (FOMO) which refers to people’s anxiety of missing social interactions or events. Other common motives include information storage, entertainment, information sharing, keeping up with trends, showing off, relationship management, and self-presentation (Lee et al., 2008; Krasnova et al., 2010; Waters & Ackerman, 2011, Cross & Shimonski, 2014; Andriyani et al., 2019). According to the 2019 CIGI-Ipsos global report, Egyptian users thought that SNSs had increased their overall quality of life (43%) and ease of communications (76%). The most important benefit of online networks is probably the social capital resulting from creating and maintaining interpersonal relationships (Ellison et al., 2007; Waters & Ackerman, 2011) However, this benefit needs users to reveal a lot of private information, which results in more risks regarding privacy violation (Yao, 2014). Individuals then have to weigh the value of privacy with the benefits of being open to others (Blatterer, 2010) and most probably, the win surpasses the loss of privacy (Mohamed & Draz, 2020) especially for teenagers and males (Youn, 2005).

Control over shared private information is extremely difficult online, since it can be abandoned without the user knowing it (Waters & Ackerman, 2011). According to the Pew Research Center survey of 2019, it was found that the majority of respondents reported having little to no control over the data that online companies collect about them and about half of them felt as if they had no control over who could access their online search terms. In recent survey, 36% of Americans said that they never read privacy policies before agreeing to them and only a minority of users who read privacy policy, mostly women and older people, said that they read them all the way through (Pew Research Center, 2019). Nevertheless, even reading the privacy policy does not seem to increase users' awareness of privacy practices on the site (Tuunainen et al., 2009). Also, although users are quite aware that the information they post is public, the full extent and possible consequences of this display may not be recognized by all (Acquisti & Gross, 2006; Lewis et al., 2008; Tuunainen et al., 2009). Furthermore, studies have shown that even when users knew about the privacy settings, only few actually made use of them and at the same time, they willingly posted large amounts of private information (Govani & Pashley, 2005; Jones & Soltren, 2005).

In a recent survey conducted by CIGI-Ipsos in 2019 worldwide regarding internet security and trust, 76% of internet users in Egypt were much more or somewhat more concerned about their online privacy compared to one year ago. According to the global digital report of January 2020, 63% of internet users in Egypt expressed concerns about how online companies use their personal data. Since it has been launched, Facebook's privacy policy and settings have often been tweaked and are regarded as overly complicated by many users. Other factors, such as online stalking, harassment, stolen personal data (Chang & Heo, 2014) and misuse of identity not necessarily by Facebook but by third parties (Prethus & Vatne, 2019) have also aroused serious concerns among Facebook users. After the "Cambridge Analytica" scandal, 55% of respondents stated that they were very concerned about the sale and use of their personal information by the Facebook Company (Gallup, 2018). However, the relationship between users' privacy concerns and actual behavior is not that simple as there is evidence that although many internet users express protective attitudes towards privacy, and willingness to apply more protective settings and share less personal information, this rarely translates to privacy-enhancing behaviors while online (Metzger, 2006; Dwyer et al., 2007; Livingstone, 2008; Tufekci, 2008; Joinson et al., 2010; Krasnova et al., 2010; Aljohani et al., 2016).

71% of Egyptians agree that social media is a significant contributor to their distrust in the internet (CIGI-Ipsos, 2019). Previous research on trusting SNSs and behaving accordingly is mixed at best. Some studies found that those who used Facebook trusted the website and therefore were less concerned about their privacy and more likely to disclose identifying information on their profiles (Metzger, 2004; Dwyer et al., 2007; Tuunainen et al., 2009) especially due to availability of control options (Krasnova et al., 2010). Other studies suggested that individuals had lower levels of trust for the use of Facebook, or the unknown others who might gain access, and thereby felt greater concern for their ability to control their information on that medium. Yet, lower levels of trust in Facebook seemed to have no significant influence on levels of informational disclosure (Christofides et al., 2009; Harris poll, 2010; Aljohani et al., 2016, Pew Center Research, 2019).

2.4 Facebook: A Privacy-Threatening App

Users indirectly pay for Facebook services when they provide details about their lives and activities which Facebook uses to attract advertisers and app makers. In the first quarter of 2020, the Facebook Company brought in $17.44 billion in ad revenue (Facebook, 2020). That puts its average revenue per user at $6.95. A major Facebook privacy-threatening incident was the infamous latest scandal of

Cambridge Analytica in March 2018 where users' private information was abused with the aim of influencing elections all over the world. On account of the scandal, a new tracking feature, named Off-Facebook Activity, was launched in January 2020 and showed information that Facebook has aggregated about users' interactions off the app over the prior 180 days. Moreover, a new whatsApp policy came into effect on February 8, 2021 indicating more alliance with Facebook over data sharing (WhatsApp, 2021). Besides commodification of Facebook-users' private information, individuals have used Facebook to harass one another (Debatin et al., 2009).

2.5 Protection of Privacy

On July 17th, 2020, President Abdel Fattah El Sisi endorsed law number 151 on the protection of personal data. The law aims to enhance the security of personal data that are being processed and kept on the internet (State Information Service, 2020). But truth be told, privacy protection in social media seems to be a figure of speech as the main target of participating in social networks is information exchange, maintenance and expansion of one's social relationships (Debatin, 2014). Although security ranked first among 28% of Egyptian respondents in the 2019 CIGI-Ipsos global survey, not everyone takes security seriously. Studies have shown that users practice poor privacy control of their information (Ellison et al, 2007; Kolek & Saunders, 2008; Debatin et al., 2009; Farag, 2015). Demographically speaking, early studies showed that frequent young users have characteristically engaged in more privacy protection behaviors than older adults who use SNSs (Madden et al., 2007; Boyd & Hargittai, 2010). While Boyd and Hargittai's (2010) research showed that there was no gender difference in how people tended to protect their privacy, Lewis et al. (2008) and Madden et al. (2013) showed that women were significantly more likely to have a private profile than did men. Andriyani et al.'s (2019) study found that teenagers who restricted access to their personal information on Facebook had a good educational background and knowledge of risks on SNSs as well.

3. METHODOLOGY

3.1 Study Design

A descriptive quantitative research design with a surveying method was used to statistically explain how privacy boundaries are coordinated on Facebook.

3.2 Selection of Participants

The current study relied on a non-random purposive sample of 487 Egyptian active Facebook users who make at least one modification to their profile at least once per week. Table 3.1 in page 10 displays sample demographic profile based on gender, generation, age, and educational level.

Table 3.1
Demographic Profile of Participants (N=487)

Demographics		*f*	*%*
Gender	**Male**	220	45
	Female	267	55
Generation	**Z (13- < 25)**	288	59
	Y (25- < 45)	128	26
	X (45-65)	71	15
Age[ii]	**13- < 18**	100	20.5
	18- < 25	188	38.6
	25- < 35	79	16.2
	35- < 45	49	10.1
	45- < 55	52	10.7
	55-65	19	3.9
Educational Level	**Basic (Primary & Preparatory)**	156	32
	Secondary/Post-secondary (General/Vocational)	114	23.4
	College	150	30.8
	Post graduate (Diploma/ Master's/PhD)	67	13.8

3.3 Data Collection Procedures

Data were collected from November 17th till December 7th, 2019 by means of an online questionnaire that was distributed via Facebook, resulting in 507 total responses. Of these, 487 responses were usable for current analysis. The questionnaire included three sections of questions designed to measure the relationships between the studied independent and dependent variables and it took about 15 minutes to complete.

3.3.1 Measures

Scales for each of the constructs were developed by averaging responses to the individual items. Higher mean scores correspond to higher degrees of the measured variable.

3.3.1.1 Facebook Use Rate

Two multiple choice questions were designed to measure the participants' overall frequency of using Facebook. Participants indicated how often they check their Facebook account per week (in days) and how much time they spend on Facebook in a typical day (in hours). Possible scores ranged from 2 to 6 (M = 4.17, SD = 1.28, α = .524).

3.3.1.2 Culture

Drawing upon Petronio's CPM theory culture criterion (2002), culture was operationalized as perceived individualism and collectivism. Both measurements were composed of 5 items each, using a 3-point Likert-type scale and adapted from Triandis and Gelfand's (1998) study. Possible scores for both subscales ranged from 5 to 15. (Individualism M = 12.69, SD = 1.73, α = .541, Collectivism M = 12.97, SD = 1.81, α = .697).

3.3.1.3 Motives for Private Disclosures

The reasons behind disclosing private information on Facebook were measured through the "Motivations for voluntary self-disclosure" measurement, adapted from Waters and Ackerman (2011). Participants were asked to rate their agreement on a 3-point Likert-type scale that consisted of 15 motive items divided into seven categories – self-presentation, relationship management, information sharing, information storage, showing off, keeping up with trends, and entertainment. A Principal Components Factor Analysis (PCA) was conducted to examine the validity and factor structure of scale items. The factorability was confirmed as the Kaiser–Meyer–Olkin measure of sampling adequacy was ≥ .5 (α > .5; p < .01). Factor loadings ranged from .64 to .85 and the lowest communality for items was .53. Internal consistencies for the factors identified were adequate, ranging from .61 to .87. The Average Variance Extracted (AVE) was greater than the minimum recommended value of .5 for all factors, ensuring that the variance explained by each factor is larger than the variance due to measurement error. Possible scores ranged from 15 to 45 (*M* = 30.21, SD = 6.12, α = .789). Using a Pearson correlation coefficient, the highest correlated factor with the overall motives indicator was *relationship management*.

3.3.1.4 Perceived Benefits/Risks

Altogether, a total of five items were used to measure the participants' degrees of perceived positive and negative outcomes of disclosing private information on Facebook. Both measurements were borrowed from Debatin et al.'s study (2009) on Facebook users' concerns regarding privacy issues. Participants were asked to rate their agreement on a 3-point Likert-type scale. Possible scores for the perceived benefits/risks subscales ranged from 2 to 6 (*M* = 5.13, *SD* = 1.07, α = .514) and 3 to 9 (*M* = 7.06, *SD* = 1.90, α = .665), respectively.

3.3.1.5 Perceived Control

Drawing upon the second principle of CPM theory, perceived control can be measured in terms of the extent to which Facebook users believe they have power over their shared private information, using five 3-point Likert-type statements adapted from the studies of Krasnova et al. (2010) and Yang et al. (2016). Possible scores ranged from 5 to 15 (M = 11.91, SD = 2.26, α = .596).

3.3.1.6 Awareness

The awareness scale was developed to measure users' knowledge of how Facebook deals with their private information. It was comprised of ten items extracted from the Facebook terms of service and data policy pages, covering Tuunainen et al's (2009) aspects about profile visibility, mechanism of privacy settings, information shared with third parties and other data related policies stated by the site. Respondents were asked to indicate whether they were familiar with each item. Possible scores ranged from 10 to 20 (M = 16.33, SD = 1.66, α = .668).

3.3.1.7 Privacy Concerns

Worries individuals have about access, misuse and dissemination of their private information or over loss of privacy as a result of information disclosure to Facebook were assessed through the "privacy violation concerns" measurement, adapted from Buchanan et al.'s (2006) study. Participants were asked to rate their agreement on a 3-point Likert scale consisting of 10 items. Possible scores ranged from 10 to 30 (M = 24.37, SD = 4.4, α = .754).

3.3.1.8 Trust

A 3-point Likert-type scale was adapted from previous studies to gauge the participants' degree of overall trust (McKnight et al., 2002; Fogel & Nehmad, 2009; Krasnova et al., 2010). The scale of trust consisted of eight items, forming two sub-scales (4 items each): trust in Facebook and trust in its members. Overall items express the beliefs that participants had about Facebook and its users possessing characteristics that inhibit them from engaging in opportunistic behaviors. Possible scores for both subscales ranged from 4 to 12 (Trust in Facebook M = 7.78, SD = 1.88, α = .54, Trust in users M = 6.93, SD = 1.87, α = .543).

3.3.1.9 Prior Invasion

Prior invasion was measured in terms of any privacy breach a Facebook user might have encountered before while using the SNS (e.g. account being hacked, shared posts being copied and reposted on other accounts, photos being uploaded on unwanted sites/pages, unapproved tags/mentions, private information being known to the public by mistake) through a yes/no dichotomous format (M = .32, SD = .02)

3.3.1.10 Use of Privacy Settings

A checklist comprised of 23 dichotomously scored items gleaned from a typical Facebook profile (i.e., whether the setting was used or not) was administered to measure respondents' self-reported usage of settings offered by Facebook to protect their personal information and manage their privacy online. Possible scores ranged from 0 to 23 (M = 8.22, SD = 6.29, α = .917).

3.3.1.11 Disclosure of Private Information

A checklist comprised of 20 dichotomously scored items was used to determine users' disclosure of private information on Facebook, and the number of items checked was converted into Information Disclosure Index (IDI) scores. Information that could be made available on Facebook users' about pages in addition to other information about daily activities, feelings, life events, etc. was used to gauge the degree to which participants disclosed their personal information. An Exploratory Factor Analysis (EFA) was conducted to categorize the items into three levels based on their sensitivity. After examining the initial 20 information items, it was found that seven items loaded highly on the first factor, with loadings ranging from .40 to .67. Four items loaded highly on the second factor, with loadings ranging from .40 to .75. The rest nine items loaded highly on the third factor, with loadings ranging from .46 to .65. Factor 1 was named "basic information", including real name, gender, birth date/year, education, workplace/professional skills, hometown/current city of residence, and relationship status. Factor 2 was named "sensitive information", including home address, mobile phone number, e-mail address, and a short personal description (bio). Factor 3 was named "highly sensitive information", including interest in men/women, family members, political views, religious views, personal photos/videos, life events, check-ins, feelings and activities. Based on the results of the EFA, each dimension of private disclosure was conceptualized as a distinct construct. Initial Eigenvalues ranged from .44 to 4.53, indicating that the factors explained 16.88%, 12.58%, and 9.16% of the variance, respectively. Possible scores for each dimension ranged from 0 to 7 (M = 4.84, SD = 1.82, α = .715), 0 to 4 (M = .7, SD = .96, α = .530), and 0 to 9 (M = 2.01, SD = 2.16, α = .765), respectively, where higher scores indicated higher levels of disclosure for all three levels of information. The order of the items was randomized in the questionnaire to minimize sequential effects.

3.3.2 Validity and Reliability

Most questionnaire items related to the overall theoretical framework and had been adopted from previous research as well as already constructed scales with slight adaptation to suit the Egyptian culture, thereby assuring good content validity. The questionnaire was also reviewed by a group of experts in various fields and they stated that the included items indeed measured what was intended to be measured, in both form and content. To insure face validity, besides expert judgment, a pre-test was also applied to a small sample of 40 respondents from both genders and of different ages, representing 10% of the total sample. Factor Analysis was used as well to assess the construct validity of some scales. As for reliability of scores, it was reflected through the internal consistency coefficient of Cronbach's alpha. Alpha values for all measures were more than .50, ranging from .514 to .917 and thereby suggesting quite good stability.

3.4 Data Analysis

Statistical analysis was performed using IBM SPSS software (version 20). Multiple Linear Regression (MLR) analysis was utilized to test the study's hypotheses. First, pair-wise correlations, using Pearson and Spearman statistical coefficients, as well as two-sample t-tests for the entire sample were examined and then only correlated variables were entered to the regression model to avoid the problem of multicollinearity. One multiple regression analysis was conducted for the use of privacy settings and three multiple regression analyses were conducted for each level of disclosed private information. Significance levels were set at .5

4. RESULTS OF FIELD STUDY

4.1 Testing the Hypotheses

Pearson and Spearman correlations (see table 4.1, page 15) as well as two-sample t-tests were estimated (see table 4.2, page 16) with only correlated/significantly different variables being entered to the regression models afterwards. The correlation and t-test results – described in the following two tables – as well as the VIF indicators from the regression tests suggested that multicollinearity was not a problem.

Table 4.1

Pearson and Spearman Coefficients for Predictors of Privacy Management Practices

	Privacy settings use	***Basic information disclosure***	***Sensitive information disclosure***	***Highly sensitive information disclosure***
Facebook use rate	.175***	.092*	-.005	.161***
Individualism	.091*	.029	.063	.085
Collectivism	-.062	.014	.057	.022
Motives	.006	.024	.014	.278***
Perceived benefits	.018	-.006	-.047	.098*
Perceived risks	.150**	.084	.004	.065
Perceived control	.319***	.012	.028	.072
Awareness	.125**	.108*	.031	.129**
Concerns	-.031	.039	.048	.048
Trust in Facebook	-.062	-.064	.096*	.057
Trust in users	-.178***	.136**	.040	.011
Age	-.005	.106*	-.013	.032
Generation	-.059	.081	.007	.032
Educational level	.128**	.193***	-.023	.115*
settings use	_	.274***	.037	.273***

** P < .05, ** P < .01, *** P < .001*

Closer inspection of significant levels in table 4.1 shows that the use of privacy-protection settings has a positive moderate correlation with perceived control over shared information, a positive weak correlation with Facebook use rate (P ≤ .001), perceived risks for private disclosures, awareness, educational level (P < .01), individualism (P < .05) and a negative weak correlation with trust in Facebook users (P ≤ .001). Positive weak correlations are found between disclosure of basic information and educational level, use of privacy-protection settings (P < .001), trust in Facebook users (P < .01), rate of Facebook use, awareness, and age (P < .05). There was a positive weak correlation between disclosure of sensitive information and trust in Facebook (P < .05). Positive weak correlations are found between disclosure of highly sensitive information and rate of Facebook use, motives for private disclosures, use of privacy-protection settings (P < .001), awareness (P < .01), perceived benefits for disclosure, and educational level (P < .05).

Table 4.2

T-test Results for Gender and Prior Invasion Predictors of Privacy Management Practices

		N	**M**	**SD**	**T- test**	**df**	**P-*value***
Privacy settings	**Male**	220	7.81	6.32	-1.280	485	.201
	Female	267	8.55	6.26			
	Invasion	157	9.72	6.22	3.684	485	.000
	No invasion	330	7.50	6.21			
Disclosure of Basic information	**Male**	220	5.00	1.85	1.671	485	.095
	Female	267	4.72	1.79			
	Invasion	157	5.16	1.77	2.653	485	.008
	No invasion	330	4.69	1.83			
Disclosure of Sensitive information	**Male**	220	.98	1.07	5.793	485	.000
	Female	267	.48	.81			
	Invasion	157	.64	1.09	-2.223	485	.027
	No invasion	330	.85	.90			
Disclosure of Highly sensitive information	**Male**	220	2.00	2.20	-.072	485	.943
	Female	267	2.02	2.13			
	Invasion	157	2.26	2.31	1.756	485	.080
	No invasion	330	1.89	2.08			

Closer inspection of the data in table 4.2 shows that a significant difference between males and females only exists in terms of disclosure of sensitive information (P < .001), and since the mean of males is higher than that of females, it can be said that males reveal sensitive private information on their Facebook accounts more than do females. There were significant differences between those who had experienced a privacy breach on Facebook and those who had not in terms of use of privacy-protection settings (P < .001), disclosure of basic information (P < .01), and disclosure of sensitive information (P < .05). By looking at the means, it is clear that victims of a prior invasion implement more privacy-protection settings and disclose more basic information and less sensitive private information.

4.1.1 Hypothesis 1: Predictors of Use of Privacy-protection Settings

Potential predictors for the behavior of using on-site privacy controls included Facebook use rate, individualism, perceived risks, awareness, prior invasion(s), perceived control, trust in Facebook users, and education. Regression estimates for those variables are presented in table 4.3, page 17.

Table 4.3

Multiple Regression Estimates for Predictors of Privacy-protection Settings Use

	Unstandardized Coefficients		*P-value*	VIF
	β	*SE*		
(Constant)	-8.650*	3.497	.014	
Facebook use rate	.479*	.211	.024	1.120
Individualism	.079	.151	.602	1.043
Perceived risks	.256	.139	.067	1.074
Awareness	.228	.157	.148	1.044
Prior invasion(s)	1.596**	.563	.005	1.058
Perceived control	.874***	.115	.000	1.025
Trust in Facebook users	-.556***	.139	.000	1.033
Education (Secondary/Post-secondary)	1.997**	.720	.006	1.419
Education (College)	1.890**	.662	.005	1.428
Education (Post graduate)	1.651*	.831	.047	1.252
Model summary				
R	.461			
R^2	.212			
Adjusted R^2	.196			
F-test	12.820			
P-*value*	.000			

* P < .05, ** P < .01, *** P < .001

Significant levels shows that trust in Facebook users is a negative predictor of use of privacy-protection settings (P < .001). Positive predictors include Facebook use rate (P < .05), being a victim to a prior invasion (P < .01), perceived control over shared information (P < .001), and education; secondary or post-secondary (P < .01), college (P < .01), and post graduate (P < .05). The overall equation was significant (P < .001) and by looking at the adjusted R^2, we can see that this model explains 19.6% of the total variance in the dependent variable of privacy-protection settings usage using only the independent variables that actually affect it.

Based on the regression results H1a, H1g, H1k, H1l, and H1o assuming that use of privacy-protection settings is predicted by Facebook use rate, perceived control, trust in Facebook users, Prior invasion, and education, respectively, are accepted while H1b, H1c, H1d, H1e, H1f, H1h, H1i, H1j, H1m, and H1n assuming that use of privacy-protection settings is predicted by individualism, collectivism, motives for disclosing information, perceived benefits, perceived risks, awareness, privacy concerns, trust in Facebook, gender, and age, respectively, are rejected.

4.1.2 Hypothesis 2: Predictors of Private disclosures

4.1.2.1 Disclosure of Basic Information.

Potential predictors for the behavior of disclosing basic information on Facebook accounts included Facebook use rate, awareness, prior invasion(s), trust in Facebook users, use of privacy settings, age, and education. Regression estimates for those variables are presented in table 4.4

Table 4.4
Multiple Regression Estimates for Predictors of Disclosure of Basic Information

	Unstandardized Coefficients			
	β	***SE***	**p-*value***	**VIF**
(Constant)	3.285***	.868	.000	
Facebook use rate	.015	.066	.823	1.154
Awareness	.074	.049	.127	1.056
Prior invasion(s)	.253*	.173	.043	1.057
Trust in Facebook users	.080	.044	.071	1.102
Privacy-protection settings use	.063***	.014	.000	1.186
Age (18- < 25)	-.244	.292	.403	3.270
Age (25- < 35)	-.409	.462	.377	2.710
Age (35- < 45)	-.569	.477	.233	3.334
Age (45- < 55)	-.407	.499	.416	3.857
Age (55 - 65)	.049	.580	.932	2.046
Education (Secondary/Post-secondary)	.644*	.292	.028	2.471
Education (College)	.653*	.390	.045	2.257
Education (Post graduate)	1.072*	.455	.019	2.989
Model summary				
R	.343			
R^2	.118			
Adjusted R^2	.093			
F-test	4.848			
P-*value*	.000			

** P < .05, ** P < .01, *** P < .001*

Significant levels shows that disclosure of basic private information is positively predicted by being a victim of a prior invasion ($P < .05$), using privacy-protection settings ($P < .001$), and education; secondary or post-secondary ($P < .05$), college ($P < .05$), and post graduate ($P < .05$). The overall equation was significant ($P < .001$) and by looking at the adjusted R^2 we can see that 9.3% of the total variance in the dependent variable of basic information disclosure can be explained by this model using only the independent variables that have an actual effect.

4.1.2.2 Disclosure of Sensitive Information

Potential predictors for the behavior of disclosing sensitive information on Facebook accounts included prior invasion(s), trust in Facebook, and gender. Regression estimates for those variables are presented in table 4.5

Table 4.5

Multiple Regression Estimates for Predictors of Disclosure of Sensitive Information

	Unstandardized Coefficients		**P-*value***	**VIF**
	β	***SE***		
(Constant)	$.633^{**}$	.195	.001	
Prior invasion(s)	$-.187^{*}$	.090	.039	1.002
Trust in Facebook	.035	.023	.125	1.015
Gender	$-.471^{***}$	.086	.000	1.017
Model summary				
R	.278			
R^2	.077			
Adjusted R^2	.071			
F-test	13.467			
P-*value*	.000			

** P < .05, ** P < .01, *** P < .001*

Significant levels shows that being a victim to a prior invasion as well as a female are negative predictors of sensitive information disclosure on Facebook ($P < .05$, $P < .001$, respectively). The overall equation was significant ($P < .001$) and by looking at the adjusted R^2 we can see that 7.1% of the total variance in the dependent variable of sensitive information disclosure can be explained by this model using only the independent variables that have an actual effect.

4.1.2.3 Disclosure of Highly Sensitive Information

Potential predictors for the behavior of disclosing highly sensitive information on Facebook accounts included Facebook use rate, motives, perceived benefits, awareness, use of privacy settings, and education. Regression estimates for those variables are presented in table 4.6, page 20.

Table 4.6

Multiple Regression Estimates for Predictors of Disclosure of Highly Sensitive Information

	Unstandardized Coefficients			
	β	***SE***	**P-** ***value***	**VIF**
(Constant)	-3.934^{***}	1.042	.000	
Facebook use rate	$.101^{*}$	.074	.045	1.124
Motives for private disclosures	$.093^{***}$	.015	.000	1.066
Perceived benefits	.035	.087	.688	1.075
Awareness	$-.099^{*}$	.055	.043	1.036
Privacy-protection settings use	$.081^{***}$	.015	.000	1.067
Education (Secondary/Post-secondary)	.372	.254	.145	1.435
Education (College)	.340	.234	.148	1.445
Education (Post graduate)	.495	.295	.094	1.276
Model summary				
R		.414		
R^2		.171		
Adjusted R^2		.106		
F-test		9.201		
P-*value*		.000		

** P < .05, ** P < .01, *** P < .001*

Significant levels shows that awareness is a negative predictor of disclosing highly sensitive information on Facebook (P < .05). Positive predictors include Facebook use rate (P < .05), motives for private disclosures (P < .001), and use of privacy-protection settings (P < .001). The overall equation was significant (P < .001) and by looking at the adjusted R^2, we can see that 10.6% of the total variance in the dependent variable of highly sensitive information disclosure can be explained by this model using only the independent variables that have an actual effect.

Based on the regression results, Facebook use rate predicted only disclosure of highly sensitive information. Therefore, H2a is partially rejected. Individualism and collectivism did not predict disclosure of any type of private information. Therefore, H2b and H2c are rejected. Motives predicted only disclosure of highly sensitive information. Therefore, H2d is partially rejected. Perceived benefits, risks, and control did not predict disclosure of any type of private information. Therefore, H2e, H2f, and H2g are rejected. Awareness predicted only disclosure of highly sensitive information. Therefore, H2h is partially rejected. Privacy concerns, trust in Facebook and its users did not predict disclosure of any type of private information. Therefore, H2i, H2j and H2k are rejected. Prior invasion predicted disclosure of basic and sensitive information. Therefore, H2l is partially accepted. Use of privacy settings predicted disclosure of sensitive and highly sensitive information. Therefore, H2m is partially accepted. Gender predicted only disclosure of sensitive information. Therefore, H2n is partially rejected. Age did not predict disclosure of any type of private information. Therefore, H2o is rejected. Finally, education predicted only disclosure of basic information. Therefore, H2p is partially rejected. Figure 4.1 shows the results of the multiple regression analysis for only significant predictors across all dependent variables.

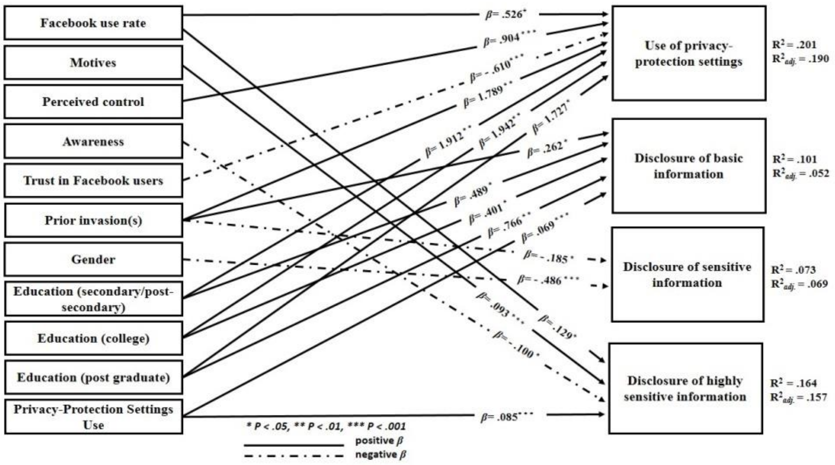

Fig. 4.1

Multiple Regression Model Results for Significant Predictors of Privacy Management Practices

5. DISCUSSION

5.1 Discussion of Findings

As predicted, higher Facebook use rate contributed to more use of on-site privacy controls supporting what has been reached by Boyd and Hargittai (2010). Moreover, Chang and Heo (2014) found that the effect of time spent on Facebook seemed to be significant on the disclosure of all types of personal information, with the greatest influence on “highly sensitive” information. This somewhat differs from the findings presented here as Facebook use rate was not found to have a significant correlation with disclosure of sensitive information and despite being correlated with disclosure of basic information, it did not predict such behavior. However, as predicted and supporting Chang and Heo (2014) findings, it contributed to more disclosure of highly sensitive information as well as more use of privacy settings. It seems logical that as individuals spend much time social networking on Facebook, the more likely they are willing to reveal more sensitive personal information and they are prone to using different privacy controls more than those who are less active.

Contrary to theoretical expectations, culture did not turn out to be a determining factor of boundary management in this study. This may be due to high scores of respondents on both cultural scales, suggesting that most people are not extreme individualistic or collectivistic but somewhere in between. Another possible explanation for this is that, in theory, culture is referred to at a national level rather than an individual one, depicting the dominant culture in a certain society. Therefore, an even larger sample nationwide may draw different results. Moreover, even if not causing it to happen, individualism being associated with using privacy controls is in line with the general claim of CPM theory that more individualistic cultures cherish privacy.

The more Facebook users are motivated by presenting themselves in a certain way, managing their social relationships, sharing experiences, keeping memories, showing off, keeping up with trends, or simply having fun, the more they divulge more highly sensitive information as seeking out these motives require a fairly high degree of information revelation/giving up a large extent of private information such as one's whereabouts, recent activities, and photos. These results are partly consistent with those of Waters and Ackerman's (2011). Information that is considered highly sensitive for disclosure on SNSs was not affected by how much users perceived benefits. These findings contradict Debatin et al.'s (2009) study as well as Youn's (2005) study. One possible explanation might be that since users' scores on both scales of awareness and perceived risks were high, it can therefore be assumed that they are well aware of the risks involved in disclosing highly sensitive personal information; therefore, they would not disclose such information, no matter how much they perceive the benefits to be. Two Facebook studies conducted by Debatin et al. (2009) and Chang & Heo (2014) support this explanation.

Although respondents' perceived risks of private disclosures were quite high, it did not drive them to share less content on their Facebook account. These findings contradicts those of Chang and Heo (2014) but corroborate those of Farag (2015) on Egyptian Facebook users. Moreover, contrary to theoretical expectations, despite being correlated to privacy settings use, perceived risks for disclosure did not cause such behavior. This may partly be explained by users' assumptions that privacy controls do not fully protect against possible negative outcomes on the site or that users get the impression that other Facebook users are at more risk for privacy breaches than they are and therefore not adjust the privacy settings to restrict access to their personal profiles (Debatin et al., 2009). As predicted, perceived control had an effect on the use of Facebook privacy settings. According to CPM, when people think they have power over what they say, they do not feel threatened or obligated to thicken their boundaries as long as they are in control. This control may be partly coming from using the site's privacy controls. The more they use privacy settings, the more control they think they have, which in turn drives them to use more settings to continuously be in control over what they post.

Awareness was not found to have a significant correlation with disclosure of sensitive information and despite being correlated with disclosure of basic information as well as use of privacy settings, it did not cause either behaviors. The findings imply that users are no stranger to how their shared private information is used by Facebook, whether or not they are prompted to protect it. The fact that scores on the awareness scale are much higher than scores on the privacy settings scale is accordant with this explanation. This is not surprising since users' management of privacy controls despite being familiar with them, as reported by prior studies was low (Ellison et al., 2007; Kolek & Saunders, 2008; Debatin et al., 2009; Joinson et al., 2010; Krämer and Haferkamp, 2014) and, based on these results, little has changed. However, as predicted, awareness contributed to a less disclosure of highly sensitive information. Respondents reported having a high level of awareness regarding how deals with its users' shared private information. That might be the reason why they did not disclose highly sensitive private information on their accounts. On the other hand, their level of awareness did not cause them to fine-tune their privacy settings. Yet, this inconsistency may be explained by the fact that the thing users were most aware of is that when a post is shared, it can be taken as a screenshot or re-shared to others across or off the site regardless of one's privacy settings. Moreover, users' awareness of the fact that Facebook has no legal liability as regards the privacy of its users' personal information may not strongly drive them to take in-depth protection measures as privacy is never really guaranteed online. These results are in consistence with those of Liu et al. (2011).

One unanticipated finding but consistent with the literature was that privacy concerns did not turn out to be significantly correlated with disclosure of any of the three types of private information or use of privacy protection settings. A previous study showed that users were willing to disclose less private information on Facebook in the future or willing to apply more protective settings (Aljohani et al., 2016). However, the actual behavior of less disclosure or more use of protection settings is rarely done as scores were low on the use of privacy settings scale within this sample. Comparison of the findings with those of other studies confirms that though reporting great concern about privacy, this does not translate into an overpowering desire to eagerly execute privacy strategies. This conclusion is in line with the findings of a great deal of the previous work in the contradicting desire to be open and SNSs users' concerns, referred to as the privacy paradox (Metzger, 2006; Dwyer et al., 2007; Livingstone, 2008; Tufekci, 2008; Joinson et al., 2010; Krämer and Haferkamp, 2014; Trepte & Reinecke, 2014; Chen & Chen, 2015; Dienlin & Trepte 2015; Kokolakis, 2017). Explanations include not needing to make any adjustments regarding privacy settings according to non-disclosers, believing that others are more susceptible to privacy violations than they are (Debatin et al., 2009), and not being aware of the problem as they claim to be, or not being knowledgeable enough about privacy settings (Acquisti & Gross, 2006; Tuunainen et al., 2009), or just relishing the instant gratifications given by the site (Taddicken & Jers, 2014).

Trust in Facebook was not found to have a significant correlation with using privacy controls, disclosing of basic or highly sensitive private information and despite being correlated to disclosure of sensitive information, it did not predict such behavior. One possible explanation for users not having such high levels of trust and thereby not being driven to disclose sensitive information is that users claimed to be quite aware of how Facebook makes use of its users' shared private information. This outcome is in accordance with that of Chang and Heo's (2014) study but contrary to that of Metzger (2004). Furthermore, the fact that many users befriend other users whom they would not consider friends away from the online environment (Govani & Pashley, 2005; Gross & Acquisti, 2005; Aljohani et al.2016), may not encourage users to tell their intimate details for the whole community of Facebook to see, depending on how one's settings are set. Lack of trust in SNS providers was also reported by Christofides et al. (2009), a Harris poll (2010), a Pew Research Center report (2019), and Aljohani et al. (2016) despite the fact that lower levels of trust did not seem to have significant influence on levels of informational disclosure across the four samples.

Trust in other Facebook users was not found to have a significant correlation with disclosure of sensitive or highly sensitive private information and despite being correlated to disclosure of "basic" information, it did not predict such behavior. However, as predicted, trust in Facebook users had a negative effect on using privacy protection settings. According to CPM theory, trust is a crucial factor in deciding to open up to other people. Therefore, managing privacy controls in a way that permits more accessibility due to trusting other Facebook members makes sense. Although respondents reported having a little more trust in Facebook than trust in other users, the overall scores on both trust scales came moderate to low as a logical result of the very high scores on the three scales of perceived risks, awareness, and privacy concerns. These results broadly support the work of other studies in this area linking concerns with trust (Fogel & Nehmad, 2009; Tuunainen et al., 2009; Krasnova et al., 2010; Lo, 2010; Chang & Heo, 2014). General lack of trust whether in Facebook or its members not leading to self-disclosure online supports previous research (Olson et al., 2005; Sheldon, 2009).

Having experienced a prior invasion was not found to be significantly correlated with disclosure of highly sensitive information. However, it was found to be a positive predictor of disclosing basic information as well as using privacy settings and a negative predictor of disclosing sensitive information. Causing disclosure of less sensitive information and more use of on-site privacy controls echo CPM's assumption that turbulence causes people to renegotiate privacy rules and adjust their disclosure and privacy management practices. What is more, use of privacy settings was not found to be significantly correlated with disclosure of sensitive information. However, as predicted, it had an effect on basic and highly sensitive private information, contributing to more disclosure of both types. Using more protective settings of Facebook may make users somewhat feel comfortable to disclose more private information as they believe such information will be secured, with the exception of sensitive information. It can therefore be assumed that as more private information is disclosed, privacy settings are put to use to protect the shared information. The reason behind most independent variables not having a significant correlation with disclosure of sensitive information compared to disclosure of the other two types of private information may be due to severe lack of sharing such information within the sample as half of the participants did not reveal their home/e-mail address, mobile number, or personal description on their Facebook accounts.

Gender was not found to be significantly correlated to use of privacy settings, supporting Boyd and Hargittai's (2010) findings while contradicting those reached by the studies of Lewis et al. (2008) and Madden et al. (2013). Gender was not found to be significantly correlated to disclosure of basic or highly sensitive information either. However, as predicted, it was found to cause differing scores on the disclosure of sensitive information scale. Females did not feel comfortable sharing their home address or mobile number on their Facebook accounts. Possible explanations for this is that females have more perceived risks of disclosing private information on their Facebook accounts and have less trust in Facebook as well as other Facebook users than do males. These results differ from those of Chang and Heo (2014). Such discrepancies can be attributed to cultural differences. However, Aljohani et al's (2016) study supports current findings as males were more likely to disclose their contact information than females and make it visible to the public. Similar conclusions were reached by Lewis et al. (2008), Fogel and Nehmad (2009) as well as Omrani and Soulie (2017) regarding Facebook female users being more cautious not to disclose private information such as telephone number and address on their profiles.

It has been suggested that young people engage in more privacy protection behaviors than adults who use SNSs (Madden et al., 2007; Boyd & Hargittai, 2010). This does not appear to be the case here. Age was not found to be significantly correlated to use of privacy settings. It was not found to be significantly correlated to disclosure of sensitive or highly sensitive information either and despite being correlated to disclosure of basic information, it did not predict such behavior. Young people's high scores on the scales of awareness and perceived risks may serve as an explanation for the current outcome. These findings are contrary to those of Blatterer (2010). Moreover, bearing in mind that generation Z comprised 59% of this study's participants, just over half this sample indicated that they accept friend requests from people they do not really know whether due to having mutual friends, or common interests. This result matches those observed in the earlier studies, indicating that a lot of users befriend other users whom they will not consider friends in a non-cyber environment (Gross et al., 2005; Govani & Pashley, 2005; Aljohani et al., 2016).

Education was not found to be significantly correlated to disclosure of sensitive information and despite being correlated to disclosure of highly sensitive information, it did not predict such behavior. However, as predicted, it was found to cause differing scores on the disclosure of basic information scale as well as the use of privacy protection settings scale. What is surprising is that higher education contributed to less use of privacy controls. Unlike previous literature, users with secondary/post-secondary level implemented more privacy strategies than those conducting post graduate studies. These differences may be partly explained by the high percentage of users within this sample who had experienced a prior privacy invasion among low-educated groups, and therefore, they are more prone to using privacy settings compared to those with higher education who had experienced fewer privacy breaches in this study. Moreover, users having a secondary/post-secondary education scored the highest rate of using Facebook, and therefore, they are more likely to be familiar with the site's privacy controls than those who spend less time social networking. However, caution should be used in describing these effects as representing trends and since the current study relied on a purposive sample, the obtained results cannot be generalized to all Egyptian Facebook users.

5.2 Study Limitations and Recommendations for Future Research

Like most studies, this study has limitations. Perhaps the biggest limitation was the absence of a clear classification of what is considered basic, sensitive, and highly sensitive information in the Egyptian culture and despite conducting an EFA to categorize respondents' chosen informational items, any items that were hardly chosen, were categorized as highly sensitive even if they are not that sensitive in nature. Second, this study did not evaluate the effect of individual motives on private disclosures. Third, as most survey-based quantitative studies do not allow for detailed answers, a comprehensive explanation for the answers could not be clarified. A number of other issues require further research such as retesting this study's current model on a different SNS or other online contexts using even different research approaches; qualitative or experimental, conducting an experimental study to compare management practices of those who have experienced turbulence and those who have not, doing some longitudinal follow-up research to examine how attitudes and behaviors of SNS users are changing over years, and measuring the effect of crises, namely Covid-19 on the depth and breadth of disclosure on social platforms.

5.3 Conclusion

This study set out to examine Facebook users' privacy management practices. To achieve this goal, the present study was designed to determine the effect of certain factors on users' voluntary disclosure of private information on their accounts as well as their use of the site's privacy controls. Multiple regression analysis revealed that higher rate of using Facebook, higher perceived control over shared private information, less trust in other Facebook users, having experienced a prior invasion, and lower education are reliable predictors of using Facebook privacy settings. The second major finding was that disclosure of private information is affected by certain factors according to the type of the disclosed information. Disclosure of basic information is caused by having experienced a prior invasion, more use of privacy settings, and higher education. Having not experienced a prior invasion and being a male contribute to disclosure of sensitive information. Disclosure of highly sensitive information is predicted by frequent use of Facebook and its privacy controls, motives for information revelation, and paucity of awareness.

REFERENCES

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies Lecture Notes in Computer Science,*36-58. doi:10.1007/11957454_3
- Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users' privacy settings & information disclosure. In Johnstone, M. (Ed.).*The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia*, 67-75. doi: 10.4225/75/58a693deee893
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Brooks/Cole, Monterey.
- Andriyani, E., Mangun, F. K., Hendiastutjik, H. K., Saidah, M., & Hidayanto, S. (2019). Privacy management of Facebook users: A study on adolescents living in west Jakarta slums. *Jurnal Komunikasi Indonesia, 8*(3), 198-207. doi:10.7454/jki.v8i3.11522
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), doi:10.5210/fm.v11i9.1394
- Blatterer, H. (2010). Social networking, privacy, and the pursuit of visibility. In H. Blatterer, P. Johnson & M.R. Markus (Eds.), *Modern privacy; Shifting boundaries, new forms.* (pp. 73-87). Basingstoke: Palgrave Macmillan.
- Boyd, D. & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday. 15* (8), 1-23. doi:10.5210/fm.v15i8.3086
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2006). Development of measures of online privacy concern and protection for use on the internet. *Journal for the American Society for Information Science and Technology, 58*(2), 157-165. doi:10.1002/asi.20459
- Chang, C., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior, 30*, 79-86. doi:10.1016/j.chb.2013.07.059
- Chen, H., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyber-psychology, Behavior, and Social Networking, 18*(1), 13-19. doi:10.1089/cyber.2014.0456
- Child, J. T. & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships.* (pp. 21-40) New York, NY: Peter Lang
- Child, J. T. (2007). *The development and test of a measure of young adult blogging behaviors, communication, and privacy management.* North Dakota State University, Fargo, ND.
- Child, J. T., & Westermann, D. A. (2013). Let's Be Facebook Friends: Exploring Parental Facebook Friend Requests from a Communication Privacy Management

(CPM) Perspective. *Journal of Family Communication, 13*(1), 46-59. doi:10.1080/15267431.2012.742089

- Child, J. T., Pearson, J. C., & Petronio, S. S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology, 60*(10), 2079–2094. doi:10.1002/asi.21122
- Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395-416. doi:10.1177/1461444808101618
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyber Psychology & Behavior, 12*(3), 341–344. doi:10.1089/cpb.2008.0226
- CIGI-Ipsos. (2019). 2019 CIGI-Ipsos global survey on internet security and trust. Retrieved July 28, 2020 from www.cigionline.org/internet-survey-2019.
- Cleary, F., & Felici, M. (2014). *Cyber security and privacy.* Cham: Springer International Publishing.
- Cross, M., & Shimonski, R. J. (2014). *Social media security: Leveraging social networking while mitigating risk.* Amsterdam: Elsevier.
- Debatin, B. (2014). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 47-60). Berlin: Springer Berlin.
- Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. doi:10.1002/ejsp.2049
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of the 13th Americas Conference on Information Systems, AMCIS 2007, Keystone, Colorado, USA, August 9-12,* 339.
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook ‘‘friends’’: Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168. doi:10.1111/j.1083-6101.2007.00367.x
- Facebook. (2020). Facebook reports second quarter 2020 results. Retrieved August 22, 2020, from https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Second-Quarter-2020-Results/default.aspx
- Farag, A. S. (2015). Thaqafat al-khsosia abr mwake’ al-tawasol al-egtema’y bayn mazaya al-efsah an al-zat wa makhateroh [Egyptian perceptions of privacy versus self-disclosure on social networking sites]. *Egyptian Journal of Public Opinion, 14*(1), 111-186.

- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160. doi:10.1016/j.chb.2008.08.006
- Gallup. (2018). Top Facebook user concerns in the United States as of April 2018. In *Statista – The Statistics Portal*. Retrieved June 3, 2019, from https://www.statista.com/statis-tics/1018760/facebook-user-concerns/
- Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Retrieved May 4, 2018, from https://www.researchgate.net/publication/228-570523
- Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review Bulletin*. *94,* 1137-1206. doi:10.31228/osf.io/c6egs.
- Gross, R., Acquisti, A., & Heinz, H. J. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society - WPES '05*. doi:10.1145/1102199.1102214
- Hofstede, G. (2005). *Culture's consequences: International differences in work-related values.* Newbury Park: Sage.
- Hofstede, G. H., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind.* New York: McGraw-Hill.
- Hofstede, G., & Bond, M. H. (1984). Hofstede's culture dimensions. *Journal of Cross-Cultural Psychology, 15*(4), 417–433. doi:10.1177/0022002184015004003
- Joinson, A. N., Reips, U., Buchanan, T., & Schofield, C. B. (2010). Privacy, trust and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. doi:10.1080/07370020-903586662
- Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. Retrieved May 2, 2018, from http://wwwswiss.ai.mit.edu/6805/studentpapers/fall05papers/facebook.pdf
- Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64,* 122-134. doi:10.1016/j.cose.2015.07.002
- Kolek, E. A. & Saunders, D. (2008). Online disclosure: An empirical examination of undergraduate Facebook profiles. *Journal of Student Affairs and Practice, 45*(1), 1-25. doi:10.2202/1949-6605.1905
- Krämer, N. C. & Haferkamp, N. (2014). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In S.Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 127-142). Berlin: Springer Berlin.
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25,* 109-125. doi:10.1057/jit.2010.6
- Lee, D. H., Im, S., & Taylor, C. R. (2008). Voluntary self-disclosure of information on the internet: A multi-method study of the motivations and consequences of disclosing information on blogs. *Psychology & Marketing, 25*(7), 692–710. doi:10.1002/mar.20232

- Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1), 79–100. doi:10.1111/j.1083-6101.2008.01432.x
- Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement, November 2011,* 61-70. doi: 10.1145/2068816.2068823
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10*(3), 393–411. doi:10.1177/1461444808089415
- Lo, J. (2010). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. Proceedings of the 16th Americas Conference on Information Systems, AMCIS 2010, Lima, Peru, August 12-15, 2010.
- Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). *Digital footprints: Online identity management and search in the age of transparency.* Washington, D.C.: Pew Internet & American Life Project.
- Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media and privacy. Retrieved April 21, 2018, from the Pew Research Center Internet and Technology https://assets.pewresearch.org/wpcontent/uploads/si-tes/14/2013/05/PIP-_TeensSocialMediaandPrivacy_PDF.pdf
- McKnight, D. H., Choudhury, V., Kacmar, C. (2002) Developing and validating trust Measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3): 334-359. doi:10.1287/isre.13.3.334.81
- Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4). doi:10.1111/j.1083-6101.2004.tb00292.x
- Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research, 33*(3), 155–179. doi:10.1177/009365020-6287076
- Mohamed, F. & Draz, A. E. (2020). Social penetration of Egyptian youth on social networking sites between conscious and unconscious. *Global Media Journal, 18*(34), 196.
- Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N. P., & Rad, F. F. (2020). User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts. *Journal of Business Research, 112*, 531-540. doi:10.1016/j.jbusres.2019.12.006
- Olson, J. S., Grudin, J., & Horvitz, E. (2005). A study of preferences for sharing and privacy. *Proceedings of CHI '05 Extended Abstracts on Human Factors in Computing Systems,* 1985-1988. doi:10.1145/1056808.1057073
- Omrani, N., & Soulie, N. (2017). Culture, privacy conception and privacy concern: Evidence from Europe before PRISM. *Proceedings of the 14th Asia-Pacific Regional*

Conference of the International Telecommunications Society (ITS), Kyoto, Japan, June 24-27, 2017.

– Papacharissi, Z. & Gibson, P. L. (2014). Privacy, sociality, and publicity on social network sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75-90). Berlin: Springer Berlin.

– Patchin, J. W. (2019, July 9). Cyberbullying victimization. *Cyberbullying Research Center*. Retrieved August 7, 2020, from https://cyberbullying.org/2019-cyberbullying-data

– Petronio, S. (2000). *Balancing the secrets of private disclosures*. Mahwah, NJ: Lawrence Erlbaum Associates.

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

– Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication, 4*(3-4), 193-207. doi:10.1080/15267431.2004.9670131

– Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13(1),* 6-14. doi:10.1080/15267431.2013.743426

– Pew Research Center. (2019, November 15). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *In Statista- The Statistics Portal.* Retrieved August 23, 2020, from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center-PI-2019.11.15-Privacy-FINAL.pdf

– Presthus, W., & Vatne, D. M. (2019). A Survey on Facebook users and information privacy. *Procedia Computer Science, 164,* 39-47. doi:10.1016/j.procs.2019.12.152

– Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication, 12*(4), 1428–1451. doi:10.1111/j.10836101.20-07.00380.x

– Robinson, S. C. (2017). Self-disclosure and managing privacy: Implications for interpersonal and online communication for consumers and marketers. *Journal of Internet Commerce, 16*(4), pp. 385–404. doi:10.1080/15332861.2017.1402637

– Sheldon, P. (2009). I'll poke you. You'll poke me! Self-disclosure, social attraction, predictability and trust as important predictors of Facebook relationships. *Journal of Psychosocial Research on Cyberspace, 3*(2), Article 1.

– Sisi endorses law on personal data protection. (2020, July 18). *State Information Service (SIS)*. Retrieved August 5, 2020, from https://www.sis.gov.eg/Story/149157/Sisi-endorses-law-on-personal-data-protection?lang=en-us

– Sophos. (2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Retrieved May 30, 2018, from https://www.sophos.com

– Taddicken, M. & Jers, C. (2014). The uses of privacy online: Trading a loss of privacy for social web gratifications? In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 143-158). Berlin: Springer Berlin.

- The Harris Poll. (2010, June 3). "Speak now or forever hold your tweets". *In the Harris Poll.* Retrieved April 13, 2018, from https://theharrispoll.com/new-york-n-y-june-3-2010-as-of-last-week-twitters-105-million-users-had-collectively-sent-15-billion-tweets
- Trepte, S. & Reinecke, L. (2014). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 61-74). Berlin: Springer Berlin.
- Triandis, H., & Gelfand, M. J. (1998). Converging measurement of horizontal and vertical individualism and collectivism. *Journal of Personality and Social Psychology, 74*(1), 118-128. doi:10.1037/0022-3514.74.1.118
- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36. doi:10.1177/0270467607311484
- Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites – Case Facebook Company. *Proceedings of the 22nd Bled e-conference, Slovenia, June 14 - 17, 2009* [paper 4]
- Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(1), 101-115. doi:10.1111/j.1083-6101.2011.01559.x
- We Are Social & Hootsuite. (2020, January 30). Digital 2020: Egypt. Retrieved June 26, 2020 from https://datareportal.com/reports/digital-2020-egypt
- Westin, A. F. (1970). *Privacy and freedom.* New York: Atheneum.
- WhatsApp. (2021, January 4). WhatsApp privacy policy. Retrieved January 22, 2021 from https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en
- Yang, K. C. C, Pulido, A., & Kang, Y. (2016). Exploring the relationship between privacy concerns and social media use among college students: A communication privacy management perspective. *Intercultural Communication Studies, 25*(2), 46-62.
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710-722. doi:10.1002/asi.20530
- Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110. doi:10.1207/s15506878jobem4901_6

[i] Drawn by the researcher

[ii] Age breakdown was derived from the global digital report's age classification of Facebook users (2020).