Examining Users' Willingness to Post Sensitive Personal Data on Social Media

O'la Hmoud Al-laymoun[1], Ali Aljaafreh[2]
Mutah University
Alkrak, Jordan

***Abstract*—Reaping the vast benefits of ubiquitous social media requires users to share their information, preferences, and interests on these websites. This research draws on communications privacy management theory and the online privacy literature to develop and validate an empirical research model testing users' willingness to share sensitive data on Facebook. The data were collected using an online survey from 569 respondents, however; 515 responses were valid for the statistical analysis. The valid data were analyzed using SMART-PLS2. The findings showed the need for attention as a significant predictor of Facebook users' willingness. Neither individual perceptions of privacy control nor privacy risks had an impact on the variable of interest. Furthermore, the evidence supported the positive impact of each of deposition to value privacy and the perceived effectiveness of Facebook's privacy policy on mitigating Facebook users' perceptions of the risks of posting their private data on the website. The paper discusses the study's theoretical and managerial implications along with its limitations.**

***Keywords*—Self-disclosure; sensitive data; Facebook policy; government regulations; privacy control; privacy risk**

I. Introduction

Facebook is the largest social network, with about 2.5 billion monthly active worldwide users as of December 31, 2019 [1]. It is not surprising that increasing numbers of people are joining Facebook, as it offers its users a wide range of benefits. According to Statista (2019), which examined the main reasons for using Facebook among 2,100 U.S citizens 15 years or older, 88% of participants reported staying in touch with family and friends as the top reason, followed by getting entertainment (33%), getting news (23%), following brands and companies (17%), and strengthening their professional networks (11%).

Unfortunately, there are risks to reaping the benefits of Facebook, as it requires its users to share information with others, creating a priceless treasure of personally identifiable information for businesses and cybercriminals to exploit [2]. For example, according to a 2018 report by Forbes.com, more than 300 million photos are uploaded to Facebook daily, and about 510,000 comments and 293,000 status updates are posted on the website every minute. Therefore, it is not surprising that Facebook represents a precious target for cybercrimes, such as privacy violations. Privacy protection is especially challenging in the era of social networking, as the world does not have or enforce the right laws and regulations to deal with a rapidly changing digital environment [3]. Privacy protection challenges are pushing lawmakers to rely more on today's empowered consumers to make the right decisions to protect themselves and their privacy while online [3]. Examples of online self-protection behaviors include managing privacy preferences and sharing information with websites that promise not to share that information with third parties [4].

Online privacy and self-disclosure on social networking sites (SNSs) and other websites have received a good deal of researchers' attention [2], [3], [5]–[11]. Yet, little has been done to understand individuals' willingness to put their sensitive information online, except by Widjaja et al. [12], which has been applied to the context of cloud storage. SNSs represent a fertile environment for this kind of research due to the increasing numbers of subscribers and the diverse potential sources of privacy threats from the website itself, as when Facebook gave Cambridge Analytica access to the data of 50 million users [13], other users, governments, or businesses. Thus, this research paper represents an attempt to fill in this gap in the online privacy literature by concentrating on the self-disclosure of sensitive data on SNSs, especially Facebook. Furthermore, this study took place in Jordan, a Middle Eastern country in which about 70% of the population uses Facebook [14]. Yet there is a dearth of research investigating Jordanian users' online privacy-related behavior. As a result, this study explores this understudied context. Specifically, this paper addresses the following research question: What factors influence Facebook users' willingness to put their sensitive information on Facebook?

II. Literature Review

A. Communication Privacy Management

This research is based on the communication privacy management theory (CPMT) proposed by Petronio [15] to study information disclosure in interpersonal relationships. Researchers have applied CPMT to understand relationships within groups, organizations, and institutions in online and face-to-face contexts [4]. CPMT has three main premises: boundary rule formation, boundary coordination, and boundary turbulence. According to CPMT, information disclosure to others has potential risks, as it makes one vulnerable to exploitation by others [15]. Nonetheless, nondisclosure has its drawbacks, as it deprives one of the benefits of disclosure, including making friends and receiving social support. Thus, when interacting with others, one goes through a risk-control assessment to weigh the rewards of disclosure and the level of control one has over the revealed information against the potential risks [16]. Based on that privacy calculus and other personality and environment-related factors, one draws a

hypothetical boundary specifying one's private space [16]. Such boundaries are regulated by rules that manage information flow in and out of the private informational space through opening (disclosing information) and closing (withholding information) boundaries. Accordingly, boundary management reflects one's perception of privacy and serves as a means of self-protection. People who impose strict control on their boundaries, by limiting revealing information to others, lower their vulnerability to exploitation and privacy concerns and vice versa [15], [17].

Furthermore, CPMT emphasizes that individuals are the owners and, as such, need to keep control of their private information even after voluntarily sharing with others who become co-owners in that case. This partnership creates a need for boundary coordination among both parties, which refers to agreeing upon privacy rules that meet the privacy expectations of the owners of the information [4]. In the case of boundary miscoordination or privacy rules violations, boundary turbulence occurs [4]. In this case, individuals seek the help of third parties by, for example, filing complaints [17].

B. Willingness to Share Sensitive Information on Facebook

The current research paper uses CPMT to investigate the role of many personal and environmental factors that motivate or hinder people from posting their private information on Facebook. The status update box on Facebook induces users to share their thoughts, media, and almost all kinds of personal information readily with their friends or even with the public [6]. According to Widjaja et al [12], there are five types of personal information representing different information sensitivity levels. These are from the least to the most sensitive: "work-related documents, personal media, personal documents, personal identity information, and specific sensitive information."

As information sensitivity increases, so does the risk associated with disclosure, making the necessary boundary management stricter [15] and lowering information disclosure [18], [19]. Research has shown that consumers' privacy concerns and willingness to share their personal information with marketers depend on information type, such that people are least open to reveal financial and personal identifier information and more willing to provide demographic and lifestyle-related information [20]. Patil and Kobsa [21] pointed out that one of the main reasons for instant messaging users' privacy concerns is content sensitivity. Metzger[4] also found that online consumers tend to protect their privacy online by withholding or falsifying sensitive information. Metzger found that consumers were most likely to withhold their financial information and information that could be linked to it, such as their social security numbers, personal contact information, and preferences, whereas they were more open to disclose their demographic information.

III. Hypothesis Development

Perceived privacy risk (PPR) is defined as the anticipated losses resulting from online disclosure of private information [16]. It is a negative belief that is expected to influence one's privacy concerns [17] as it stems from the potential risk of being a victim of opportunistic behavior [22] resulting from information misuse [17]. Generally speaking, people weigh the benefits and risks of disclosure when participating in social exchange situations and, as a result, choose to disclose if the benefits outweigh the risks or withhold if the opposite is true [5]. Many studies have examined the consequences of PPR. For example, it has had a negative association with consumers' willingness to transact online [23]. In the same context, Dinev and Hart [22] found it had a negative relationship with willingness to provide personal information to participate in online transactions. In addition, Millham and Atkin [10] found that the higher one's perception of the risks resulting from disclosing information on online social networks, the greater the sense of information ownership and responsibility, which, in turn, leads to lower willingness to reveal sensitive personal information on these networks. In line with the previous studies, we posit the following:

H1: Perceived privacy risk has a negative impact on users' willingness to post sensitive personal information on Facebook.

Perceived privacy control (PPC) is defined as one's perception of the ability to control the collection, dissemination, and the resulting use of one's private information [16]. In general, when individuals do not have that control or when they are not aware of the subsequent uses of their information, they tend not to disclose [24]. According to CMPT, individuals are the owners of their personal information and, thus, they need to keep it under their control [12]. Indeed, a recent study has shown that most online consumers are worried about how companies handle their information and seek more control over the ways businesses process that information [20] to mitigate the possible risks of disclosure [24]. In the context of e-commerce, Phelps et al. [20] found that consumers' information control had a positive association with online shopping intention; however, the researchers also reported that intention was higher when consumers were asked to submit lifestyle or demographic information than when they were asked to submit financial or personal identifier information. In another study by Benson et al. [9], users' control over personal data had a negative relationship with information disclosure in the context of SNSs. On Facebook, the privacy and security threats are not limited to the misuse of published content by the website. One's network friends and even strangers could also be sources of all kinds of violations, making publishing one's private data a sensitive matter. Indeed, Zlatolas et al. [8] found that privacy control had no significant impact on the self-disclosure behavior of Facebook users. Thus, based on the aforementioned studies, we propose the following:

H2: Perceived privacy control has no impact on users' willingness to post sensitive personal information on Facebook.

We are extending CMP theory by adding the need for attention construct, which can impact online user behavior, such as posting malicious comments [25] and online political content generation and consumption [26]. In the context of social media, users face information overload as they receive all kinds of digital content from their online friends and from strangers. Thus, they have to be selective in the content they

pay attention to and interact with. To stand out from the crowd and increase the attention their posts receive from others, people with a high need for attention might tend to have a high frequency of online content creation and to select content that is likely to attract others. We expect posting sensitive data on Facebook to serve that goal by providing material unique to the individual instead of presenting general information. Indeed, in a longitudinal study, Hawk et al. [27] found that adolescents' attention-seeking motives had a positive relationship with their self-disclosure on social media. Thus, we propose the following:

H3: Need for attention has a positive impact on users' willingness to post sensitive personal information on Facebook.

Disposition To Value Privacy (DTVP) is an inherent personal need to maintain one's private space and control the flow of information outside that space [16], [17]. DTVP is analogous to the privacy orientation construct in CPMT [12]. According to Widjaja et al.[12], people who score high on DTVP value privacy more and perceive higher privacy and security risks in disclosure than those who score low on that construct. For example, Patil and Kobsa [21] found a relationship between DTVP and instant messaging users' privacy concerns. The positive relationship between DTVP and PPR has also found support in several other contexts, such as cloud-based storage applications [12], e-commerce, SNSs, financial, and healthcare sites [16], [17]. Thus, in line with the extant literature, we postulate the following:

H4: Disposition to value privacy has a positive impact on perceived privacy risk.

The online environment is risky, and information disclosed online could be misused by, for example, being sold to third parties without consent. Once individuals provide their information to a website, it becomes hard for them to remove it or even to control its subsequent use [28]. Information asymmetries increase the complexity of that situation by limiting individuals' awareness of the organization's information practice and whether their collected information may be misused [29]. Per CMPT, once one shares one's information with others, they become co-owners. Both parties need to negotiate the owners' privacy expectations regarding how the co-owners will use and handle that information and who else can access it in a process called boundary coordination [30]. In online contexts, a website could address its customers' privacy concerns and signal that it is a trustworthy custodian of their information by using institutional privacy assurances, defined as interventions taken by the company to protect and keep the privacy and safety of its customers' information[15] [30], such as privacy policies [16] and notices [29].

Privacy policies are mechanisms informing individuals of the subsequent uses of their information, the safety measures and privacy rules used to protect their information from different kinds of misuse, and the ways available to them to keep their information accurate and up-to-date [16]. They communicate whether, how, and when consumers' private information will flow out the collective boundary after being disclosed, helping users to decide whether their acceptable privacy rules and the organization's rules align [4] and enhancing users' overall regard for and trust of the organization [5]. In the context of e-commerce, Jarvenpaa et al. [23] found that the higher consumers' trust in a website, the lower the perceived risk of purchasing from that website. Chellappa and Sin [31] pointed out that individuals' usage of online personalization services had a positive relationship with their trust in the online merchant; thus, they suggested that vendors need to use trust-building methods and tools if they want to collect and capitalize on their consumer's data. Furthermore, in some cases, when users were informed that fair information practices are in place to protect their information, privacy concerns did not differentiate those who were willing to have their information used for profiling from those who were not [32]. Interestingly, in an experimental setting of e-commerce, Jensen et al. [33] found that the existence of privacy policies impacted participants' behavior, although they were rarely consulted. Thus, we propose the following hypothesis:

H5: The perceived effectiveness of Facebook privacy policy a) negatively impacts perceived privacy risks and b) positively impacts perceived privacy control.

Sometimes, privacy policies and other forms of institutional privacy assurances used by organizations to assure their customers that their information will be kept confidential and safe are not adequate to meet those customers' expectations. According to CPMT, when boundary coordination fails, boundary turbulence occurs. Boundary turbulence results from privacy violations, lack of boundary coordination, or conflicting privacy rules used by different people [5]. In that case, consumers tend to turn to other forms of institutional privacy assurances, such as industry self-regulation and government regulations, to protect their privacy [12].

The literature on privacy has emphasized government legislation as one of the main approaches individuals use to maintain their online and offline privacy [12]. Like other countries, Jordan has special legislation in place to combat online crimes. The Cybercrimes Unit in Jordan's Public Security Department is the official party that Jordanians turn to if they become victims of cybercrimes. Widjaja et al. [12] found that the perceived effectiveness of government regulations in enhancing users' perceived privacy control had no impact on the perceived cost of putting sensitive data on cloud-based applications. However, in line with CPMT, we expect it to have a positive influence on PPC and a negative association with PPR. Thus, we propose the following:

H6: The perceived effectiveness of government regulations a) negatively impacts perceived privacy risks and b) positively impacts perceived privacy control.

IV. Research Methodology

A. Data Collection and Instrument Development

A survey was employed to collect the primary data from Facebook users in a large public university in Jordan. The data were collected using a questionnaire developed on Google Forms and attached with a cover letter, assuring the confidentiality of research participants and outlining the study's primary purpose. A pilot study was conducted with

seven undergraduate students, and, as a result, minor modifications were made to the initial version of the questionnaire. The questionnaire was posted to 32 teams on Microsoft Teams, corresponding to 32 different classes taught on that application during the lockdown in Jordan during the "COVID-19 pandemic". Professors encouraged their students to participate in the study. Participation was voluntary, and no incentives were available to the research subjects. The data collection process took about a month and a half. The total number of received responses was 526, of which 515 were retained for further analysis while the rest were dropped from the study due to inconsistent answers. The demographic characteristics of the research sample are outlined in Table I.

TABLE I. DEMOGRAPHIC CHARACTERISTICS OF THE SAMPLE

Measure	Item	Frequency	(%)
Gender	Male	153	29.7
	Female	362	70.3
Facebook Daily hours	Less than 1 hour	128	24.9
	1 to less than 2 hours	90	17.5
	2 to less than 3 hours	97	18.8
	3 to less than 4 hours	72	14.0
	4 to less than 5 hours	41	8.0
	More than 5 hours	87	16.9
Age	18-22	249	48.3
	23.26	126	24.5
	27-30	39	7.6
	31-34	23	4.5
	35-38	28	5.4
	39-42	34	6.6
	More than 42	16	3.1
Education	Bachelor's	401	77.9
	Master's	87	16.9
	PhD	27	5.2

B. Measures

A questionnaire with a 5-point Likert-type scale (ranging from 1 = "strongly disagree" to 5 = "strongly agree") was employed to collect the data. All measures were adopted from previous studies and adapted as needed to achieve the purpose of this research. Willingness to post sensitive personal data on Facebook measures Facebook users' readiness to make their private data available for other users on the website. The construct adopted from [12] asked the research subjects to indicate their willingness level to put five different types of personal information on the social network. Perceived privacy risk measures one's cognitive assessment of the potential privacy threats associated with personal data availability on Facebook. The variable was adapted from [17] and consisted of four items. Perceived privacy control reflects one's evaluation of the ability to manage what to post on Facebook, who can view that content, and controlling how Facebook can use that data. The variable was measured using four items, and it was adopted from [17]. The need for attention reflects one's desire to be noticed and appreciated by others. Five items adopted from [25] were used in this study. However, one of the items ("I don't like people who do not respond to my post on Facebook") was dropped for not loading well on the latent variable. Disposition to value privacy was adopted from [17]. This variable used three items to measure the predisposition to value privacy online and offline; however, one item ("Compared to others, I tend to be more concerned about threats to my information privacy") was dropped as it did not load well on the construct. The perceived effectiveness of Facebook policy refers to individuals' evaluation of Facebook's commitment and ability to protect its users' privacy. The construct was measured using three items adopted from [12]. Finally, the perceived effectiveness of government regulations is defined as the perception of the research subjects of the ability of the Cybercrimes Unit in Jordan to handle any privacy violation incidents they might face. Three items were adopted from [12], and one item developed by the researchers was used to measure the variable.

V. RESULTS

A. Measurement Model

The measurement model was evaluated using the convergent validity and discriminant validity of the survey. The research instrument's reliability was assessed using two measures: the composite reliability (CR) and Cronbach's alpha. The recommended threshold for both measures is 0.7 or above; however, a value of 0.5 is considered the minimum acceptable value [34]. According to the results presented in Table II, the composite reliability ranges between 0.868 and 0.943 substantially exceed the recommended criterion. In regard to Cronbach's alpha, the values for the seven constructs were between 0.698 and 0.92. Based on these results, we feel confident in the high internal consistency of the research instrument. The research validity was tested using discriminant validity and convergent validity [35]. Average variance extracted (AVE) and factor loadings were employed to assess the convergent validity. The requirement of having an AVE of 0.5 or more has been satisfied, as Table II shows. Furthermore, all factor loadings exceeded the desired threshold of 0. 7. To ensure discriminant validity, each indicator's factor loading should be higher on the factor it measures than any other factor. This condition was also met. Thus, convergent validity and discriminant validity have been established.

B. Structural Model

The findings of the PLS-SEM analysis are summarized in Table III and Fig. 1. The results indicate that three out of the seven hypotheses were statistically accepted. The analysis results showed that Disposition to value privacy (β =0.456, t-value=4.1944) had a significant positive impact on Perceived Privacy Risk, therefore; H1 has been confirmed. Also, the results showed that Need for Attention strongly affected Willingness to post sensitive data on Facebook (β =0.299, t-value=3.346), thus, the results confirmed the positive impact hypothesized in H4. Finally, the SEM analysis revealed that Facebook Policy was a significant predictor for Privacy Control (β =0.446, t-value=4.440), thereby supporting H8.

TABLE II. OVERVIEW OF QUALITY CRITERIA AND FACTOR LOADINGS

Construct	Items	Factor loadings	AVE	CR	Cronbach α
The perceived effectiveness of government regulations	CCU1	0.8865	0.806	0.943	0.920
	CCU2	0.8734			
	CCU3	0.92			
	CCU4	0.9119			
Disposition to value privacy	DP1	0.8717	0.768	0.868	0.698
	DP2	0.8812			
The perceived effectiveness of Facebook privacy policy	FBPE1	0.8468	0.774	0.911	0.854
	FBPE2	0.9081			
	FBPE3	0.8845			
Need for attention	NA1	0.8084	0.708	0.906	0.862
	NA2	0.8896			
	NA3	0.881			
	NA4	0.784			
Perceived privacy control	PC1	0.7889	0.701	0.802	0.858
	PC2	0.8479			
	PC3	0.8762			
	PC4	0.8352			
Perceived privacy risk	PR1	0.8372	0.671	0.890	0.838
	PR2	0.8787			
	PR3	0.7358			
	PR4	0.8203			
Willingness to post sensitive personal data	W1	0.7188	0.504	0.802	0.678
	W2	0.7106			
	W3	0.703			
	W4	0.7085			

TABLE III. PLS COEFFICIENT PATH ANALYSIS

Hypotheses	Beta (β)	t-value	results
H1. Perceived privacy risk -> Willingness to post	0.167	1.4444	rejected
H2. Privacy Control -> Willingness to post	0.071	0.6399	rejected
H3. Need for Attention -> Willingness to post	0.299	3.3468	Accepted
H4. Disposition to privacy -> Perceived privacy risk	0.456	4.1944	Accepted
H5.a. Facebook policy -> Perceived privacy risk	0.078	0.7231	rejected
H5.b. Facebook policy -> Privacy Control	0.446	4.4404	Accepted
H6.a. Government regulations -> Perceived privacy risk	0.058	0.5661	rejected
H6.b. Government regulations -> Privacy Control	0.190	1.56	rejected
H6.a. Government regulations -> Perceived privacy risk	0.058	0.5661	rejected
H6.b. Government regulations -> Privacy Control	0.190	1.56	rejected

[a.] Note: Explained variance proportion R^2 of Willingness to post = 0.118, Explained variance proportion R^2 of Perceived privacy risk = 0.214, Explained variance proportion R^2 of Privacy Control = 0.318.

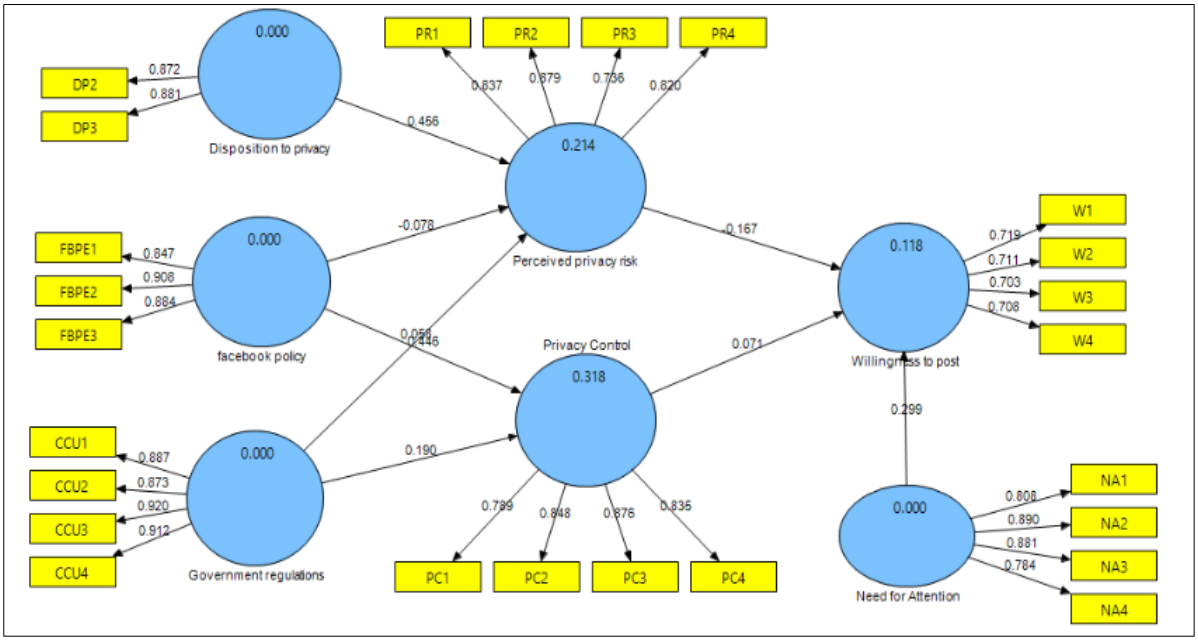

Fig. 1. PLS Path Analysis.

VI. Discussion

This study is an attempt to add to the literature on online privacy management. Specifically, we are looking at Jordanian Facebook users' willingness to post their sensitive personal data on Facebook. The study leverages the extant literature on privacy to develop and to empirically examine a research model combining CPMT and the need for attention construct to understand better what motivates or hinders users from revealing their private data on SNSs.

The results showed that the proposed model accounts for about 11.8% of the dependent variable, indicating that more investigation is still needed in this regard. In general, the results provided reasonable evidence of the role of the psychological need for attention as a motivator feeding individuals' readiness to share their sensitive data with their Facebook friends and even with strangers. This result signals the crucial influence of one's inner needs in shaping one's acceptance of specific behaviors. In line with our expectations, the study revealed no impact on perceived privacy control on the willingness to post private data on Facebook. Although this result confirms the results of some earlier studies [8], it contradicts other studies that either found positive or negative relationships between the aforementioned variables. This finding suggests that further research is needed to clarify the nature of the relationship between the variables and what moderators, if any, influence it. Furthermore, contrary to our expectations, perceived privacy risks had no significant relationship with individuals' willingness to share. This result is consistent with the findings of [36]. This may in part be attributable to the culture. Although people cognitively assess the likely risks of online self-disclosure and their control over their data, they might perceive the rewards of doing so as overweighing the risks. For instance, in a collectivistic culture like Jordan, people are more prone to social influence than in individualistic cultures. Social influence can impact the intention of self-disclosure on social media positively [36].

Moreover, the study found a positive influence for DTVP on PPR. In terms of institutional privacy assurances, two forms were investigated in this paper: the effectiveness of Facebook policy and the effectiveness of government privacy regulations. Consistent with the previous studies in this research area, the empirical evidence found that Facebook policy enhanced Facebook users' sense of control over their data posted on Facebook. However, our study found no significant impact of that policy on the perceptions of risks. These findings imply that policies play a role in assuring users that they are the owners of their data and that Facebook empowers them to manage it, yet these policies are running behind in terms of addressing and educating people about the potential vulnerabilities of being victims of privacy violations. With regard to the perceived effectiveness of government regulations, we found no support for its impact on PPC or PPR. Our findings are partially consistent with the study by [12]. They found no impact on the perceived effectiveness of government regulations in the context of cloud-based storage applications on PPR. However, it contradicts the evidence reported in the literature on the impact on PPC. This may be because the laws and regulations we have today are still not adequately addressing the fast-changing and very diverse online security and privacy violation domains [3]. People might doubt governments' ability to give them complete control over their online information and its subsequent uses. They also might question how effective these regulations would be.

The empirical evidence from the study has several important implications for researchers and practitioners alike. In terms of practical implications, finding a significant impact of the need for attention on people's willingness to put their sensitive data on Facebook highlights the importance of

understanding social media users' psychological needs. The data online surfers post on SNSs represents a priceless treasure that businesses, governments, and other parties can mine to understand and target their audiences better. Thus, investing in big data, data mining, and other technologies to understand online users becomes a necessity. Moreover, Facebook needs to continue improving its filtering, recommendations, privacy management, and other tools to create safe and secure social environments that induce people to network and make friendships with others without being afraid of privacy and security threats. The study also makes theoretical contributions. First of all, while most research on online self-disclosure pays little attention to information sensitivity [12], especially when examining social media, this study takes that important matter into consideration. As indicated in previous research, people were more likely to self-disclose when they were asked to reveal low sensitivity information. In addition, to the best of the researcher's knowledge, the current study is one of the few empirical studies that has applied CPMT to investigate online user behavior in Jordan and the Arab world in general.

VII. Limitations and Future Research

Generally speaking, research studies can suffer from different kinds of drawbacks. This paper is no exception. First of all, users' perceptions of risk and, in turn, their willingness to reveal private data on Facebook could be a function of whether their account is private or public. No differentiation between account types has been made in this study. This factor could be studied in future research. Second, although this study focused on Facebook, its main premises could be extended to other social media applications. Third, it would be interesting to examine the research model in different cultures and to measure individuals' perceived willingness to post and their actual behavior.

VIII. Conclusion

Drawing on the communications privacy management theory and the online privacy literature, we developed a research model investigating users' willingness to share sensitive data on Facebook. A survey was used to collect the data from Facebook users in Jordan. The posited model explains about 11.8% of users' willingness to post personal data on the network. The results showed the need for attention as a significant predictor of Facebook users' willingness, whereas neither individual perceptions of privacy control nor privacy risks had a significant impact. The preliminary empirical evidence from this study sheds light on the importance of the psychological needs in shaping one's online behavior. It also opens the doors for future research to explore this novel area of research.

References

[1] Facebook, "Facebook Reports Fourth Quarter and Full Year 2012 Results," 2020.

[2] A. Vishwanath, W. Xu, and Z. Ngoh, How people protect their privacy on facebook: A cost-benefit view, vol. 69, no. 5. 2018.

[3] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, "Exploring motivations for online privacy protection behavior: Insights from panel data," Communic. Res., p. 0093650218800915, 2018.

[4] M. J. Metzger, "Communication privacy management in electronic commerce," J. Comput. Commun., vol. 12, no. 2, pp. 335–361, 2007.

[5] M. J. Metzger, "Privacy, trust, and disclosure: Exploring barriers to electronic commerce," J. Comput. Commun., vol. 9, no. 4, p. JCMC942, 2004.

[6] E. E. Hollenbaugh and A. L. Ferris, "Facebook self-disclosure: Examining the role of traits, social cohesion, and motives," Comput. Human Behav., vol. 30, pp. 50–58, 2014.

[7] A. Gruzd and Á. Hernández-García, "Privacy concerns and self-disclosure in private and public uses of social media," Cyberpsychology, Behav. Soc. Netw., vol. 21, no. 7, pp. 418–428, 2018.

[8] L. N. Zlatolas, T. Welzer, M. Heričko, and M. Hölbl, "Privacy antecedents for SNS self-disclosure: The case of Facebook," Comput. Human Behav., vol. 45, pp. 158–167, 2015.

[9] V. Benson, G. Saridakis, and H. Tennakoon, "Information disclosure of social media users," Inf. Technol. People, 2015.

[10] M. H. Millham and D. Atkin, "Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors," New Media Soc., vol. 20, no. 1, pp. 50–67, 2018.

[11] L. Yu, H. Li, W. He, F.-K. Wang, and S. Jiao, "A meta-analysis to explore privacy cognition and information disclosure of internet users," Int. J. Inf. Manage., vol. 51, p. 102015, 2020.

[12] A. E. Widjaja, J. V. Chen, B. M. Sukoco, and Q.-A. Ha, "Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study," Comput. Human Behav., vol. 91, pp. 167–185, 2019.

[13] K. Wagner, "Here's how Facebook allowed Cambridge Analytica to get data for 50 million users - Vox," Mar. 2018.

[14] Statista, "• Jordan: share of Facebook users 2017 | Statista," 2017.

[15] S. Petronio, "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples," Commun. theory, vol. 1, no. 4, pp. 311–335, 1991.

[16] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view," ICIS 2008 Proc., p. 6, 2008.

[17] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," J. Assoc. Inf. Syst., vol. 12, no. 12, p. 1, 2011.

[18] P.-C. Sun, R. J. Tsai, G. Finger, Y.-Y. Chen, and D. Yeh, "What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction," Comput. Educ., vol. 50, no. 4, pp. 1183–1202, 2008.

[19] S. Yang and K. Wang, "The influence of information sensitivity compensation on privacy concern and behavioral intention," ACM SIGMIS Database DATABASE Adv. Inf. Syst., vol. 40, no. 1, pp. 38–51, 2009.

[20] J. Phelps, G. Nowak, and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information," J. Public Policy Mark., vol. 19, no. 1, pp. 27–41, 2000.

[21] S. Patil and A. Kobsa, "Uncovering privacy attitudes and practices in instant messaging," in Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work, 2005, pp. 109–112.

[22] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," Inf. Syst. Res., vol. 17, no. 1, pp. 61–80, 2006.

[23] S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, "Consumer trust in an Internet store," Inf. Technol. Manag., vol. 1, no. 1–2, pp. 45–71, 2000.

[24] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents-measurement validity and a regression model," Behav. Inf. Technol., vol. 23, no. 6, pp. 413–422, 2004.

[25] H.-M. Kim and G.-W. Bock, "The Role of Attention and Neutralization in Posting Malicious Comments Online," 2018.

[26] K. Shim, "Does Fear of Isolation Disappear Online? Attention-Seeking Motivators in Online Political Engagement," Media Commun., vol. 7, no. 1, pp. 128–138, 2019.

[27] S. T. Hawk, R. J. J. M. van den Eijnden, C. J. van Lissa, and T. F. M. ter Bogt, "Narcissistic adolescents' attention-seeking following social rejection: Links with social media disclosure, problematic social media use, and smartphone stress," Comput. Human Behav., vol. 92, pp. 65–75, 2019.

[28] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The value of privacy assurance: an exploratory field experiment," Mis Q., pp. 19–33, 2007.

[29] G. R. Milne and M. J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," J. Interact. Mark., vol. 18, no. 3, pp. 15–29, 2004.

[30] A. Aljaafreh, A. Al-Ani, R. Aladaileh, and R. Aljaafreh, "Initial trust in internet banking service in Jordan: Modeling and instrument validation," J. Theor. Appl. Inf. Technol., 2015.

[31] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma," Inf. Technol. Manag., vol. 6, no. 2–3, pp. 181–202, 2005.

[32] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," Organ. Sci., vol. 10, no. 1, pp. 104–115, 1999.

[33] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of Internet users: Self-reports versus observed behavior," Int. J. Hum. Comput. Stud., vol. 63, no. 1–2, pp. 203–227, 2005.

[34] Hajli, M. N., "A Study of the Impact of Social Media on Consumers",

[35] International Journal of Market Research, Vol. 56, No. 3, 2014, pp. 387-404.

[36] Hair, B., & Black, J. W. Babin & Anderson, "Multivariate Data Analysis", 2010.

[37] Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites. Internet Research, 25(2), 279-299.