sustainability

MDPI

Article

Understanding the Key Antecedents of Users' Disclosing Behaviors on Social Networking Sites: The Privacy Paradox

Byoungsoo Kim [1] and Daekil Kim [2,*]

[1] School of Business, Yeungnam University, 280 Daehakro, Gyeongsansi 38541, Korea; kbsyu@yu.ac.kr
[2] School of Communications and Media, Seoul Women's University, 621 Hwarangro, Nowon-Gu, Seoul 01797, Korea
* Correspondence: chris74@swu.ac.kr; Tel.: +82-53-810-2730

Received: 30 May 2020; Accepted: 23 June 2020; Published: 24 June 2020

Abstract: This study explored the formation mechanisms of users' disclosing behaviors from the perspectives of the privacy paradox. The theoretical framework incorporates perceived control over personal information and subjective norms into the privacy calculus model. The proposed theoretical framework was empirically tested using survey data collected from 350 Facebook users. The findings show that users' intention to disclose personal information has a marginally significant effect on users' disclosing behaviors. The analysis results reveal that privacy concerns negatively affect the intention to disclose personal information while they are not significantly related to users' disclosing behaviors. This study found that perceived control over personal information plays a significant role in enhancing trust in social network site (SNS) providers, users' intention to disclose personal information, and users' disclosing behaviors. Moreover, perceived control over personal information mitigates the level of privacy concerns. Several implications for research and practice are described.

Keywords: social network service; privacy paradox; perceived control; privacy calculus model

1. Introduction

Social network sites (SNSs) are an effective communication tool to keep in touch with people and develop social capital [1,2]. Given the rapid development of mobile networks such as WIFI and 5G, users can access mobile applications anytime, anywhere and share a variety of content such as photos and videos. SNS providers such as Instagram and Facebook have grown rapidly through real-time communication and information sharing. Due to the recent influence of COVID-19, communication through SNSs is drawing more attention. Because of the various advantages of SNSs and the market environment, the global number of Facebook users is expected to reach 1.69 billion [3]. However, SNS security, access controls, and privacy protection are notably weak by design [4,5]. Moreover, as cases of privacy abuse and unwarranted access to private information have increased, SNS users have become more aware of these privacy threats [6–8]. From the perspective of SNS providers, collecting and analyzing users' personal information enables the provision of customized advertisements and personalized services. Cambridge Analytica, a political data firm hired by U.S. President Donald Trump, gained access to voters' private information from more than 50 million Facebook users without their consent [9]. Such incidences of privacy invasion discourage SNS users from providing personal information to the service provider. But it is still a debatable question whether users' intention to disclose personal information promotes users' disclosing behaviors. According to the privacy paradox, the effect of users' disclosing intention on disclosing behaviors was not significant due to the inconsistency between behavioral intention and actual behaviors [10–12]. Several studies

on SNSs have shown that privacy concerns negatively affect users' disclosing intention to disclose personal information, but have no significant impact on actual disclosing behaviors [11,12]. In this vein, this study examines the formation mechanisms of users' disclosing behaviors to verify the privacy paradox.

Users' decision to disclose personal information on SNSs is mainly based on the privacy calculus model [13,14]. The privacy calculus model asserts that users compare potential benefits and costs (risks) that either enable or inhibit their disclosing behaviors when they allow SNS providers to access their personal information [15,16]. If SNS users feel that they can gain benefits, such as self-expression, entertainment, and personalized services, by disclosing personal information, then they are likely to relinquish some level of their privacy while using SNSs. Several studies have empirically demonstrated that the privacy calculus model is well fitted for examining SNS users' disclosing behaviors [14,17]. Several studies on SNSs have investigated the effects of trust beliefs, privacy concerns, and perceived benefits in users' decision-making processes in the context of SNSs [18,19]. In line with prior studies on the privacy calculus model, this study posits that user decisions on SNSs are a product of perceived benefits, trust in the SNS provider, and privacy concerns [18,19]. SNS users provide demographic information such as gender, birth date, and residential address while creating an SNS profile. However, privacy concerns are more serious in SNS environments due to their unique attributes. This is because SNSs involve a different set of social interactions and information-sharing activities compared to other service platforms [4,5]. In particular, SNSs collect and gather enormous amounts of personal information. For example, SNS users consciously reveal such personal information as their political views, favorite quotations and movies, and music preferences when communicating with their friends. Thus, privacy concerns are considered a key impediment to disclosing personal information, as providing personal privileged information on SNS involves a certain degree of privacy risk. However, several studies have shown that privacy concerns have a negative effect on users' intention to disclose personal information while they have no effect on users' disclosing behaviors [10–12]. This means that despite the high concerns about privacy invasions, there is a contradiction in not doing anything to protect privacy or rather disclosing personal information to the service provider [20,21]. Thus, this study examines the discrepancy in the impact of perceived benefits, privacy concerns, and trust in a service provider on users' intention to disclose personal information and disclosing behaviors.

Several studies on SNSs highlight the importance of information control over personal information in developing users' disclosure behaviors [5,22]. Information control is associated with the capacity users have to control information released by SNSs [15,16]. Information control related to collecting, storing, and utilizing users' personal information serves as the key factor in enhancing their disclosing behaviors and decreasing the level of privacy concern. Phelps et al. [23] showed that the lack of control over personal information amplifies users' privacy concern. This study investigates the role of subjective norms on users' disclosing behaviors. Subjective norms are defined as the degree to which users perceive their friends', colleagues', and relatives' approval of their SNS usage and disclosure [18,24]. Given subjective norms, users experience social pressure to frequently access and share their diary or photos to confirm the expectations of significant reference individuals [25,26]. Thus, this study clarifies the role of information control over personal information and subjective norms in developing SNS users' disclosure behaviors.

This study contributes to the literature on SNSs in several ways. The objective of this study is to explore the formation mechanisms of users' disclosing behaviors from the perspectives of the privacy paradox. It examines the discrepancy in the impacts of antecedents on users' intention to disclose personal information and disclosing behaviors. Users' disclosing behaviors are shaped by three main components: the privacy calculus model, perceived control over personal information, and subjective norms. Structural equation modeling (SEM) was used to analyze a sample of 350 Facebook users. The analysis results offer several theoretical and practical insights that can aid SNS providers in understanding the privacy paradox phenomenon of users' disclosing behaviors.

2. Theoretical Background and Research Model

2.1. Privacy Calculus Model and Privacy Paradox

Social exchange theory determines social interaction as behavior underlying the assessment of benefits and costs that people expect from others [27]. The overall assessment of perceived benefits and costs induces social interactions with others when potential benefits exceed potential costs. Individuals sacrifice a certain degree of privacy in exchange for utilitarian and hedonic benefits [28]. In the context of privacy, the privacy calculus model is suggested based on this cost–benefit structure. Individuals evaluate the potential benefits and negative consequences with respect to disclosing personal information and using a service [29]. This implies that individuals sacrifice a certain degree of privacy in exchange for utilitarian and hedonic benefits [27,29]. Individuals are likely to disclose personal information if they perceive the overall benefits of disclosure to be balanced at least with their assessed risks [14,17]. On the benefit side, anticipation of benefits such as perceived usefulness and perceived enjoyment motivates users to disclose information and enhance their continuance intention [5,22]. However, on the cost side, privacy concerns discourage users from continuing to use the service and sharing their personal information [15,16]. In addition, this model considers trust belief as a confidence belief that can positively influence the disclosure of personal information and continuance intention.

Privacy is defined as "the freedom to choose one's own movement across the boundary that distinguishes one's self as being and functioning alone versus one's self as a separate individual interacting and functioning with others" [29]. According to the communication privacy management theory, individuals pursue a balance between the disclosure and production of their private and personal information [30–32]. This is a significant issue because online companies rely on the ability to collect large amounts of personal information about users to provide personalized products and services [17,29]. A number of information systems (IS) researchers have highlighted the importance of individual privacy concerns regarding personal information in an online environment [15,33]. Privacy concerns reflect online users' concerns regarding inappropriate data collection, secondary use, ownership, accuracy, and access without consent. A 2014 survey showed that 90% of respondents are worried about losing control over how personal information is gathered and used in the online environment [34]. A 2014 survey showed that 80% of respondents in the U.S. were not comfortable with the collection and unauthorized secondary use of personal information by advertisers [35]. These surveys have consistently indicated that people are very concerned with the ways online companies use their personal information. Indeed, users with high concern for information privacy are likely to take protective actions to reduce the risks, such as refusing to provide personal information, providing inaccurate information, or ending use of the website. Wu [33] noted that users act on a more complex set of mechanisms than the simple trade-off when they decide to disclose their personal information on SNSs. Kroll and Stieglitz [34] investigated the effects of perceived control, trust in provider, and perceived privacy risk on disclosing behaviors. Moreover, they empirically tested the effect of privacy-related nudges on perceived control, trust in provider, and perceived privacy risk. Thus, several studies have found that information privacy concerns are a critical barrier to disclosing personal information and a key reason behind protective behavior [2,36]. Most prior studies on privacy concerns have focused on the effects of information privacy in the context of e-commerce, commercial websites, and SNSs [15,16,37]. However, some studies on the privacy paradox have shown the relationship between users' disclosing intentions and their actual disclosure is weak or not related at all [20,21]. Several studies showed that privacy concerns influence a negative attitude towards certain services, but rarely affect actual behavior [11,12].

2.2. Research Model and Hypotheses

This study investigates the difference in the effects of the key antecedents on SNS users' intentions to disclose personal information and their disclosing behaviors from the perspectives of the privacy

paradox. This study postulates that users' disclosing behaviors are affected by three distinctive components: the privacy calculus model, perceived control over personal information, and subjective norms. The theoretical model is shown in Figure 1.

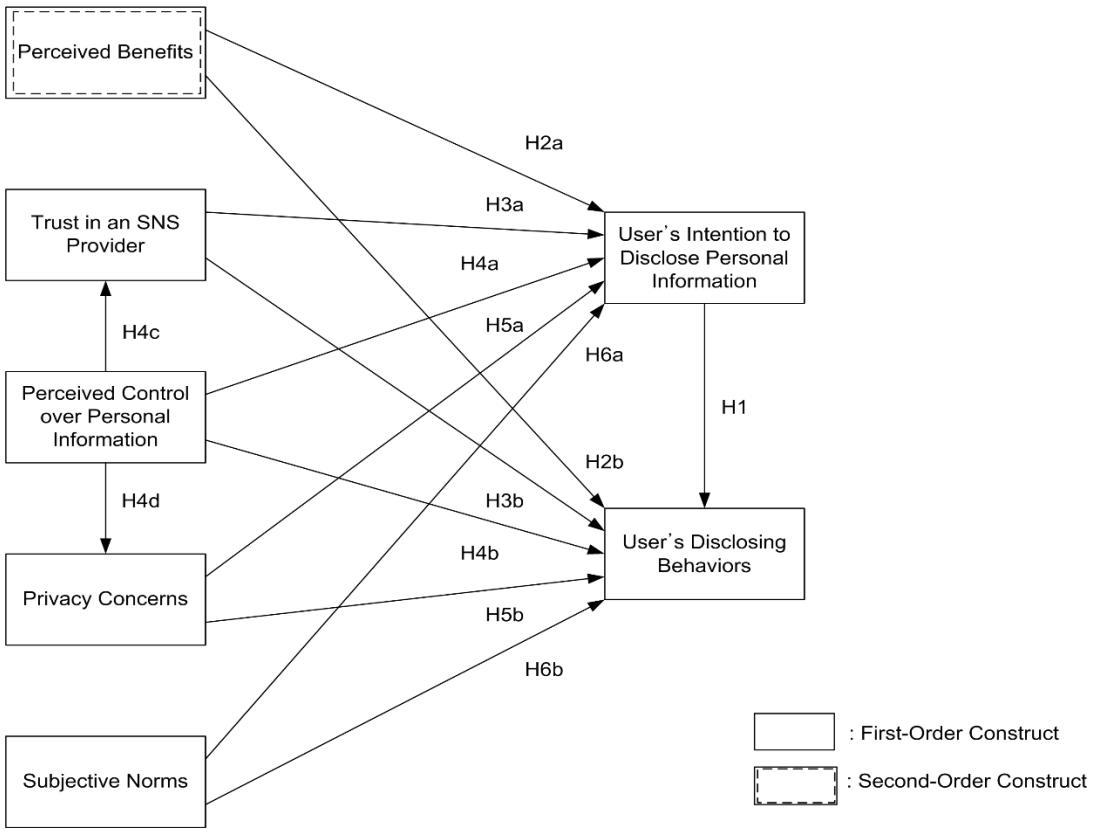

Figure 1. Research Model.

2.2.1. Users' Intention to Disclose Personal Information

Behavioral intention is defined as a user's conscious plan to carry out a particular behavior. The TRA (theory of reasoned action) and the TPB (theory of planned behavior) have shown the significant and strong effect of behavioral intention on actual behavior [38,39]. Several studies have identified behavioral intention as the salient predictor of actual behaviors based on rational decision-making processes [39,40]. However, with respect to privacy, users' disclosing intention is not predictive of disclosing behaviors because of antecedents that affect disclosing intention and disclosing behaviors independently [20,21]. To check the paradoxical dichotomy, this study investigated the effect of users' disclosing intention on disclosing behaviors.

Hypothesis 1 (H1). *Users' intention to disclose personal information positively influence users' disclosing behaviors.*

2.2.2. Perceived Benefits

The uses and gratifications theory (UGT) explains why individuals seek to choose certain media to gratify their needs and motives [41]. It assumes that people actively seek out a specific communication medium that meets their psychological needs. Users are conscious and purposive media selectors while fulfilling their personal and psychological needs. Gratification is distinct from user satisfaction because it focuses on the fulfillment of an individual's personal, psychological, and social goals through media communication [42,43]. The UGT has been widely applied to understand users' motivations in

the context of traditional media, such as TV and newspapers, as well as interactive media, such as blogs and SNSs. Gratification can be divided into three categories: content gratification, process gratification, and social gratification [44]. Users receive content gratification when they choose to use a certain medium for content, information, or materials. Process gratification refers to users' satisfaction with regard to the fun and pleasurable experience of using the medium itself. Social gratification is conceptualized as the degree to which users believe that using a medium gratifies their need for social interaction. In particular, in the SNS environment, social gratification is considered a prominent factor that facilitates users' interactions and interpersonal communication among members on SNSs. Several studies on SNSs have examined why individuals choose SNSs over other media alternatives and continue to use them [42,45,46]. The UGT suggests that users are more likely to continue to engage on SNSs if their content, process, and social gratification are fulfilled. For example, Hew [45] revealed that students are satisfied with maintaining current relationships, bonding with new friends, engaging in self-expression, and seeking entertainment through the use of SNSs. Ku et al. [46] identified information seeking, amusement, relationship maintenance, style, and sociability as five major forms of gratification as motives behind using SNSs such as Facebook and Instagram. Huang et al. [47] emphasized that fulfilling users' social needs (e.g., social interaction, bonding with friends, and maintaining social relationships) is a fundamental form of gratification from using SNSs. James et al. [48] categorized the primary forms of gratification from SNS as the formation and maintenance of relationships, information-seeking, self-expression, and pleasing others. When SNS users are gratified with their online and mobile interaction experiences, they are more likely to engage in post-adoption behaviors such as continuance and information-disclosing behaviors. Ifinedo [49] posited purposive value, maintaining interpersonal connectivity, entertainment value, self-discovery, and social enhancement as the main forms of gratification while engaging with SNSs. Therefore, to reflect the aforementioned categories of gratification, this study developed a research model by using three categories: social gratification (network management), process gratification (entertainment), and content gratification (self-expression). This study investigated the effects of perceived benefits on users' disclosing intention and disclosing behaviors.

Hypothesis 2a (H2a). *Perceived benefits positively influence users' intention to disclose personal information.*

Hypothesis 2b (H2b). *Perceived benefits positively influence users' disclosing behaviors.*

2.2.3. Trust in an SNS Provider

Trust refers to users' willingness to be vulnerable to some actions based on the expectation that others will exhibit ethical behaviors [50]. A number of studies have verified the vital role of trust in users' decision-making in various IS contexts [14,18]. Indeed, a lack of trust in a service provider would be a critical barrier to using an IS or sharing personal information with the service provider [21,51]. Several studies on SNSs have suggested that trust is a social and relational component that is a key enabler of SNS use and sharing of private information with the service provider [15,52]. In the context of computer-mediated communications such as SNSs, trust serves as a significant factor in mitigating users' perception of privacy invasion and abuse [53,54]. Therefore, trust in an SNS provider can lead to favorable consequences via the reduction of uncertainty about information abuse and illegal information aggregation. In particular, SNS users expose or disclose sensitive personal information when registering for the service and communicating with their relatives through the service. As SNS providers can access users' personal sensitive information without the consent of how and where their information is being used, trust in an SNS provider encourages them to disclose their personal information. Therefore, if SNS users consider the SNS provider to be reliable and trustworthy, then they are likely to form a positive attitude and share their personal information without anxiety.

Hypothesis 3a (H3a). *Trust in an SNS provider positively influences users' intention to disclose personal information.*

Hypothesis 3b (H3b). *Trust in an SNS provider positively influences users' disclosing behaviors.*

2.2.4. Perceived Control over Personal Information

Perceived control over personal information refers to individuals' belief in one's ability to manage personal information about oneself [55]. Although the element of control is embedded in the concept of privacy concerns, Xu et al. [17] insist that perceived control is different from privacy concerns. Perceived control is related to the ability of the use of dissemination of personal information and limiting others' access to their personal information [23]. Several studies on SNSs posit perceived control over personal information as a factor that alleviates privacy concerns and facilitates disclosing behaviors [15,16]. Xu and Gupta [29] showed that perceived privacy control mitigates users' perception of privacy and invasion, which in turn impacts their disclosing behaviors and participation in online activities. Dinev et al. [16] revealed that perceived control over information significantly influences perceived privacy in the context of Web 2.0. They showed that users tend to have a lower degree of privacy concern regarding the disclosure of personal information, as they have a reasonable level of control over their information on Web 2.0 services. Hanjli and Lin [5] identified perceived control over information as a facilitator to share users' personal information on SNSs. High perceived control over information increases users' desire to disclose self-expressive information because they are less worried about the invasion of privacy. Thus, most SNS providers offer users control over personal information by giving them an option to change privacy settings and select the level of information-sharing [56]. These privacy settings help limit access to disclosed personal information by third parties and other users. Thus, the following hypothesis posits that perceived control over personal information increases users' trust in an SNS provider, users' intention to disclose personal information, and disclosing behaviors. Moreover, perceived control over personal information would decrease perceived privacy concerns.

Hypothesis 4a (H4a). *Perceived control over personal information positively influences users' intention to disclose personal information.*

Hypothesis 4b (H4b). *Perceived control over personal information positively influences trust in an SNS provider.*

Hypothesis 4c (H4c). *Perceived control over personal information negatively influences privacy concerns.*

Hypothesis 4d (H4d). *Perceived control over personal information positively influences users' disclosing behaviors.*

2.2.5. Privacy Concerns

Privacy concerns regarding private information are a prominent barrier to decisions related to the disclosure of personal information and uploading of photographs by users [7,8]. Information-related privacy concerns have been considered as one of the most important issues in the context of SNSs because of the uncertainty regarding the privacy and security of personal information [2,5]. Privacy concerns include the unauthorized sharing of personal information, disclosure of customers' political behavior, and spamming through personalized advertisements [2,13,53]. When SNS users perceive their informational privacy to be under threat, they become reluctant to use SNSs and disclose their personal information. In this regard, several studies on SNSs have shown that privacy concerns are likely to lower consumer willingness to disclose user information. Although users are becoming less sensitive to disclosing their private information on SNSs, they are still concerned about the safety of

significant information and perceive privacy risks [54]. When users register on some SNSs, they must provide sensitive personal information such as alma mater, residential address, and workplace [2,5,17]. SNS providers can collect and analyze users' personal information to offer personalized services and customized advertisements without their consent. SNS providers can also sell users' private or personal data to marketing companies, financial institutions, and government agencies for commercial gain. Several studies on SNSs have shown that privacy concerns are one of the most critical barriers in facilitating the disclosure of personal information by users [2,5,7]. However, although users with concerns regarding the abuse of private information tend to hesitate in disclosing personal information, the reverse effect can be observed. Some users share personal information seemingly without any hesitation due to the discrepancy between privacy concerns and the actual behaviors of users [20,21]. Joinson et al. [11] showed that privacy concerns negatively affect users' intention to disclose personal information while they have no significant effect on users' disclosing behaviors. This study is expected to show that privacy concerns are negatively related to users' intention to disclose personal information while they are not significantly associated with users' disclosing behaviors.

Hypothesis 5a (H5a). *Privacy concerns negatively influence users' intention to disclose personal information.*

Hypothesis 5b (H5b). *Privacy concerns have no significant effect on users' disclosing behaviors.*

2.2.6. Subjective Norms

The TPB is a well-established framework elucidating user behavior in a variety of IS contexts [38,39]. It regards subjective norms as a vital factor that affects users' decision-making. Social norms refer to users' perception of whether significant individuals such as friends, family, and other relatives would approve or disapprove of their behavior. Venkatesh and Brown [57] revealed that social norms serve as a key enabler of users' decision to use a certain IS. In the SNS environment, social norms are defined as the degree to which users would approve of significant individuals using SNS. Social norms are related to social pressure from friends, relatives, and colleagues concerning users' continuance intention and disclosure of personal information on SNSs [18,24]. Kim and Min [18] also confirmed the explanatory power of social norms in the context of SNSs. According to the social influence theory, if a majority of important relatives recommend users' usage of and disclosure of information on SNSs, then they are more likely to accept the suggestions and disclose their information. Given social norms, users recognize social pressure to frequently disclose their information as conforming to the expectations of significant individuals [25]. Thus, it is expected that subjective norms have a positive impact on users' intention to disclose personal information and their disclosing behaviors.

Hypothesis 6a (H6a). *Subjective norms positively influence users' intention to disclose personal information.*

Hypothesis 6b (H6b). *Subjective norms positively influence users' disclosing behaviors.*

3. Research Methodology

3.1. Instrument Development

This study involved a self-administered survey questionnaire via an online survey agency. All questions were derived from a previous study to validate the measurements in IS, marketing, and hospitality. The measurement items were modified to suit the context of Airbnb. The survey items consisted of three parts, which were as follows: (1) users' disclosure and usage behaviors with regard to Facebook; (2) users' privacy concerns, trust in a service provider, perceived control, and subjective norms; and (3) users' demographic information. In the first part, respondents were asked about information and usage patterns of Facebook in terms of the frequency of information disclosure and use of Facebook. If the respondents did not use Facebook in the last three months, our survey was designed

to end; otherwise, they could move on to the next part, which covered users' privacy concerns, trust in a service provider, perceived control, and subjective norms regarding Facebook. The questionnaire was measured on a seven-point Likert scale ranging from 1 ("strongly disagree") to 7 ("strongly agree"). In the last part of the survey, users were asked about their demographic information such as age, gender, and education. Before conducting the survey, the measurement items were checked by three researchers in IS, service marketing, and hospitality domains. The final measurement items reflect some minor problems in the questionnaire's ambiguity, wording, and content.

Users' disclosing behaviors were from measures by Kim et al. [58]. Users' intention to disclose personal information was adapted from the instruments created by Min and Kim [2]. Network management, enjoyment, and self-expression were measured by scales adapted from Ifinedo [49]. Drawing on Hajli and Lin [5], we measured perceived control over personal information using four items. Privacy concerns were assessed with scales developed by Malhotra et al. [55]. Three questions measuring subjective norms were derived from Kim and Min [18].

A pilot study (N = 25) was performed to validate the measurements. The reliability of all measurement items was confirmed by evaluating the values of Cronbach's alpha, composite reliability (CR), and average variance extracted (AVE). All Cronbach's alpha and CR values were higher than 0.7, which is the acceptable cutoff value for reliability. Moreover, all AVE values exceeded 0.5.

3.2. Subjects and Data Collection

The theoretical framework was empirically tested by the use of data gathered from the online-based survey. A cross-sectional survey was conducted for users who had used Facebook in the last three months. We cooperated with an online survey agency that has a number of panels in South Korea. The online link to access the questionnaire was distributed to its panels via e-mail. Only after answering all questions on each page could respondents proceed to the next page. After deleting insincere responses, 350 responses were utilized for the next analysis. Table 1 presents the demographic information of the final respondents. Among the final samples, 54.3% were male and 45.7% were female. The mean age of the final sample was 35.4 with a standard deviation of 9.7. The final respondents' usage period ranged from 1 to 60 months, with a mean usage period of 18.31 months and a standard deviation of 11.67.

Table 1. Profile of respondents.

Demographics	Item	Subjects (N = 350)	
		Frequency	Percentage
Gender	Male	190	54.3
	Female	160	45.7
Age	Less than 30	118	33.7
	31~40	112	32.0
	More than 40	120	34.3
Main Usage Device	PC	144	41.1
	Notebook	23	6.6
	Smart Phone	171	48.9
	Smart Pad	12	3.4

4. Research Results

In this study, the measurement model and the structural model were analyzed using the partial least squares(PLS) method. The PLS method is a component-based technique that has some benefits in terms of minimal restrictions on sample size and residual distributions [59,60]. The method is well suited for complex research models with a lot of constructs, including formative constructs. As this study involves the handling of formative indicators and a number of constructs, it was conducted as a

two-stage SEM. In the first stage, we assessed the convergent validity, reliability, and discriminant validity of the measurement items. The second tested the structural model.

4.1. Measurement Model

A confirmatory factor analysis was conducted to evaluate convergent validity, reliability, and discriminant validity. To test for convergent validity, factor loadings were investigated. Convergent validity was satisfied because the item loadings exceeded 0.60 [61]. To test the reliability of the constructs, the composite reliability (CR) and average variance extracted (AVE) values were calculated. Reliability is acceptable if the CR values are higher than 0.70, the AVE values are higher than 0.50, and the Cronbach's alpha values are higher than 0.70 [62]. As shown in Table 2, all CR, AVE, and Cronbach's alpha values exceeded the recommended threshold values. In terms of Cronbach's alpha, all values were higher than 0.70, which is the recommended threshold. Third, to examine discriminant validity, the AVE values of the individual constructs were compared with the shared variances between constructs. In Table 3, the diagonal values of the matrix, which are the square root of the AVE values of our constructs, exceeded the correlations between the construct and the other constructs, thus satisfying discriminant validity.

Table 2. Scale reliabilities.

Construct		Item	Mean	St. Dev.	Factor Loading	CR	AVE
Disclosing Behaviors		DEB1	2.709	1.787	0.917	0.914	0.78
		DEB2	4.731	1.520	0.799		
		DEB3	2.900	1.800	0.929		
Intention to Disclose Personal Information		IDPI1	3.949	1.496	0.931	0.953	0.836
		IDPI2	3.983	1.529	0.946		
		IDPI3	3.974	1.537	0.927		
		IDPI4	3.603	1.637	0.851		
Perceived Benefits	Network Management	NET1	4.686	1.42	0.906	0.937	0.831
		NET2	4.951	1.333	0.923		
		NET3	4.814	1.297	0.906		
	Enjoyment	ENJ1	4.829	1.166	0.912	0.953	0.836
		ENJ2	4.840	1.201	0.920		
		ENJ3	4.889	1.224	0.906		
		ENJ4	4.843	1.233	0.919		
	Self-Expression	SEL1	4.594	1.254	0.906	0.950	0.827
		SEL2	4.531	1.286	0.897		
		SEL3	4.689	1.286	0.930		
		SEL4	4.709	1.242	0.903		
Trust in an SNS Provider		TSP1	4.217	1.202	0.873	0.938	0.752
		TSP2	4.417	1.277	0.882		
		TSP3	4.223	1.361	0.864		
		TSP4	4.32	1.181	0.877		
		TSP5	4.123	1.242	0.84		
Privacy Concerns		PCO1	5.386	1.068	0.863	0.936	0.786
		PCO2	5.449	1.109	0.879		
		PCO3	5.451	1.125	0.909		
		PCO4	5.389	1.14	0.895		
Perceived Control over Personal Information		PCPI1	4.251	1.314	0.899	0.954	0.838
		PCPI2	4.206	1.364	0.920		
		PCPI3	4.069	1.380	0.921		
		PCPI4	4.020	1.399	0.920		
Subjective Norms		SUI1	4.660	1.22	0.861	0.930	0.816
		SUI2	4.594	1.312	0.923		
		SUI3	4.600	1.331	0.925		

Table 3. Correlation matrix and discriminant assessment.

	1	2	3	4	5	6	7	8	9
1. Disclosing Behaviors	0.883								
2. Intention to Disclose Personal Information	0.356	0.915							
3. Network Management	0.321	0.356	0.912						
4. Enjoyment	0.428	0.471	0.597	0.914					
5. Self-Expression	0.402	0.507	0.623	0.788	0.909				
6. Trust in an SNS Provider	0.364	0.613	0.428	0.526	0.595	0.867			
7. Privacy Concerns	0.091	−0.185	0.155	0.21	0.172	−0.020	0.887		
8. Perceived Control over Personal Information	0.400	0.609	0.451	0.516	0.532	0.690	−0.130	0.915	
9. Subjective Norms	0.406	0.525	0.637	0.69	0.756	0.597	0.162	0.537	0.903

Note: Diagonal values are the square root of AVE.

4.2. Structural Model and Hypothesis Testing

An SEM was conducted to evaluate the hypothesized paths among the constructs through PLS. A bootstrap resampling method with 500 resamples was conducted to check the significance of the hypotheses within the research model. The analysis results are shown in Figure 2.

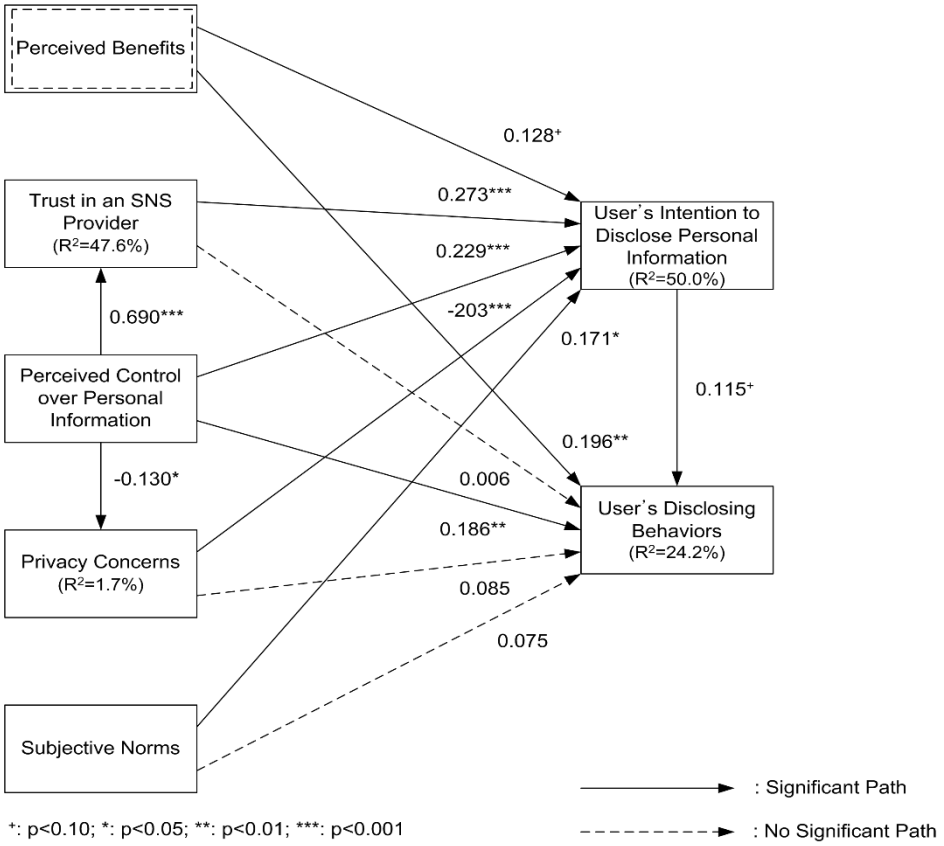

Figure 2. Analysis results.

Consistent with expectations, users' intention to disclose personal information has a marginally significant effect on users' disclosing behaviors, thus supporting H1. Perceived benefits have a significant influence on both users' intention to disclose personal information and users' disclosing behaviors, thus supporting H2a and H2b. Trust in an SNS provider has a significant influence on users' intention to disclose personal information while it has no significant effect on users' disclosing intention. Hence, H3a is supported and H3b is not supported. Perceived control over personal information is positively associated with trust in SNS providers, users' intention to disclose personal information, and users' disclosing behaviors. However, perceived control over personal information is

negatively related to privacy concerns. Hence, H4a, H4b, H4c, and H4d are supported. Privacy concerns negatively affect intention to disclose personal information while they are not significantly related to users' disclosing behaviors. Therefore, H5a and H5b are supported. Subjective norms are significantly associated with users' intention to disclose personal information while they are not significantly related to users' disclosing behaviors. Therefore, H6a is supported but H6b is not supported. The theoretical model explained 24.2% of the variance in users' disclosing behaviors and 50.0% of the variance in users' intention to disclose personal information. Table 4 summarizes the analysis results.

Table 4. Summary of the results.

	Cause	Effect	Coeffi.	t-Value	Significant
H1	Users' Intention to Disclose Personal Information	Users' Disclosing Behaviors	0.115	1.647	Marginally Significant
H2a	Perceived Benefits	Users' Intention to Disclose Personal Information	0.128	1.679	Marginally Significant
H2b	Perceived Benefits	Users' Disclosing Behaviors	0.196	2.557	Significant
H3a	Trust in an SNS Provider	Users' Intention to Disclose Personal Information	0.273	4.686	Significant
H3b	Trust in an SNS Provider	Users' Disclosing Behaviors	0.006	0.073	Not significant
H4a	Perceived Control over Personal Information	Users' Intention to Disclose Personal Information	0.229	3.709	Significant
H4b	Perceived Control over Personal Information	Users' Disclosing Behaviors	0.186	2.551	Significant
H5a	Perceived Control over Personal Information	Trust in an SNS Provider	0.690	17.694	Significant
H5b	Perceived Control over Personal Information	Privacy Concerns	−0.130	2.089	Significant
H5c	Privacy Concerns	Users' Intention to Disclose Personal Information	−0.203	5.556	Significant
H5d	Privacy Concerns	Users' Disclosing Behaviors	0.085	1.403	Not significant
H6a	Subjective Norms	Users' Intention to Disclose Personal Information	0.171	2.170	Significant
H6b	Subjective Norms	Users' Disclosing Behaviors	0.075	0.916	Not significant

5. Discussion and Implications

5.1. Theoretical and Practical Implications

The analysis results showed that users' intention to disclose personal information weakly affects disclosing behaviors. Although the TPB and the TRA assume a strong relationship between behavioral intention and actual behaviors, the relationship between users' disclosing intention and disclosing behaviors could be weak due to the privacy paradox phenomenon. In line with prior studies on the privacy paradox, our results revealed the marginal relationship between users' disclosing intention and disclosing behaviors.

Second, this study examined the discrepancy in the impacts of key antecedents on users' intention to disclose information and disclosing behaviors based on the privacy calculus model. This study shows that user decisions to disclose personal information are mainly explained by the privacy calculus model. It empirically demonstrates that the privacy calculus model serves as a well-fitting research model to investigate SNS users' disclosing behaviors. This study confirms the salience of perceived benefits in disclosing behaviors. As users can benefit from using SNSs, such as maintaining social interactions and experiencing positive feelings, perceived benefits play an important role in their disclosing behaviors. The results indicate that "perceived benefits" is a high-order construct formed through network

management (β = 0.261, t = 23.417), enjoyment (β = 0.429, t = 35.98), and self-expression (β = 0.429, t = 41.551). This second-order construct offers a more detailed description of multiple perspectives of perceived benefits, thus leading to an in-depth understanding of the influence of key factors on users' disclosing behaviors in the context of SNSs. This study clarifies the salient role of trust in an SNS provider in enhancing users' intention to disclose personal information. In line with the results of previous studies, users' intention to disclose personal information is largely explained by trust in SNS providers. This result implies that greater trust in SNS providers may enhance users' intention to disclose personal information on SNSs. These results imply that the effect of trust in an SNS provider on users' disclosing behaviors was not significant due to the inconsistency between behavioral intention and actual behaviors. However, the analysis results showed that trust in an SNS provider is not significantly related to users' disclosing behaviors. Norberg et al. [12] showed that trust in an SNS provider indirectly influences users' disclosing behaviors through behavioral intention.

Third, this study systematically illustrates how perceived control over information influences users' disclosing behaviors in the context of SNSs from a psychological perspective. Perceived control over personal information may be efficient and effective in countering users' privacy concerns. Consistent with previous studies, our research verifies the significance of perceived control over information in both users' intention to disclose information and their disclosing behaviors. This study clarifies the positive impacts of perceived control over personal information on users' intention to disclose personal information and disclosing behaviors. Specifically, it shows that perceived control over personal information has a significant influence on users' disclosure intention, (1) indirectly through trust in SNS providers and privacy concerns and (2) by directly influencing the disclosure intention. Perceived control over personal information increases the level of trust in SNS providers, which in turn influences their disclosing intention and behaviors. Consistent with our expectations, perceived control over personal information mitigates SNS users' privacy concerns. According to the information boundary theory [17,29], users develop personal informational boundaries based on risk and control assessment. If users perceive themselves as having little control over the disclosed information, they are likely to have higher levels of privacy concerns and lower levels of participation in SNS activities.

Next, this study found that privacy concerns have a negative influence on users' intention to disclose personal information. Consistent with the privacy calculus model, privacy concerns serve as a key impediment to users' intention to disclose personal information. The results imply that SNS users are concerned that shared personal information will be misused, which weakens the willingness to disclose personal information. A user survey on Facebook reported that 87.8% of users revealed their birth date, 50.8% shared their current residence, and a majority disclosed their relationship status, political views, and other interests [6]. Such open personal information on SNSs increases the possibilities of criminal abuses and cybercrimes. Thus, privacy concerns have an important role in reducing users' level of disclosing intention. The results imply that SNS users are concerned that shared personal information will be misused, which weakens the willingness to disclose personal information. Consistent with the privacy calculus model, privacy concerns serve as a key impediment to disclosure of personal information. However, the analysis results found the privacy concerns are not related to users' disclosing behaviors. In line with prior studies on the privacy paradox, privacy concerns significantly influence users' intention to disclose, but they rarely translate into actual disclosing behaviors.

Lastly, the results of this study support the TRA by verifying the significant role of subjective norms in explaining users' intention to disclose personal information on SNSs. This study finds that subjective norms have a significant influence on users' intention to disclose information. Heirman et al. [63] also showed that perceived social pressure exerted by others increases the exposure to their opinions. Moreover, they found that subjective norms are the most important enabler in explaining users' intention to disclose personal information. However, subjective norms are not directly related to users' disclosing behaviors. In line with our findings, Kim and Min [18] showed that subjective norms do

not induce users to disclose information. This study confirmed the indirect effect of perceived social pressure exerted by others on users' disclosing behaviors through disclosing intention.

5.2. Limitations and Future Research Directions

This study has some limitations that must be addressed for future research. First, data were collected and tested from only a single country, that is, South Korea. Some studies on SNSs have found an important role played by cultural characteristics such as Hofstede dimensions in the formation of disclosing behaviors [64,65]. Thus, future studies should conduct a survey in various countries to check the validity and generality of the results. Second, although this study reveals the moderating role of gender in disclosing behaviors, other variables such as demographic variables or usage patterns could play a similar role. Future studies should investigate new moderators in the formation of disclosing behaviors. Finally, this study investigates the factors affecting users' intention to disclose personal information at a static point. To provide more insights for researchers and practitioners, it is better to examine the dynamic effects of factors on the disclosure of personal information. Further research needs to conduct a longitudinal survey to investigate the dynamic effects of perceived control over personal information, subjective norms, and the privacy calculus model in disclosing personal information.

Author Contributions: Conceptualization: B.K.; Formal Analysis: B.K. and D.K.; Writing—Original draft preparation: D.K.; Writing—Reviewing and editing: B.K.; Funding Acquisition: D.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the 2020 Yeungnam University Research Grant.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Boyd, D.M.; Ellison, N.B. Social network sites: Definition, history, and scholarship. *J. Comput. Mediat. Commun.* **2007**, *13*, 210–230. [CrossRef]
2. Min, J.; Kim, B. How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *J. Assoc. Inf. Sci. Technol.* **2015**, *66*, 839–857. [CrossRef]
3. Number of Monthly Active Facebook Users Worldwide as of 1st Quarter 2020. Available online: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (accessed on 24 June 2020).
4. Sun, Y.; Fang, S.; Hwang, Y. Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability* **2019**, *11*, 3311. [CrossRef]
5. Hajli, N.; Lin, X. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *J. Bus. Ethics* **2016**, *133*, 111–123. [CrossRef]
6. Gross, R.; Acquisti, A. Information revelation and privacy in online social networks (the Facebook case). In Proceedings of the Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005; pp. 71–79.
7. Acquisti, A.; Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Proceedings of 6th Workshop on Privacy Enhancing Technologies*; Golle, P., Danezis, G., Eds.; Robinson College: Cambridge, UK, 2006; pp. 36–58.
8. Mohamed, N.; Ahmad, I.H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Comput. Hum. Behav.* **2012**, *28*, 2366–2375. [CrossRef]
9. Trump-Linked Firm Cambridge Analytica Collected Personal Information from 50 Million Facebook Users without Permission. Available online: https://www.businessinsider.com/cambridge-analytica-trump-firm-facebook-data-50-million-users-2018-3 (accessed on 24 June 2020).
10. Barth, S.; de Jong, M.D.T. The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telem. Inform.* **2017**, 1038–1058. [CrossRef]
11. Joinson, A.N.; Reips, U.D.; Buchanan, T.; Paine Schofield, C.B. Privacy, trust, and self-disclosure online. *Hum. Comput. Interact.* **2010**, *25*, 1–24. [CrossRef]

12. Norberg, P.A.; Horne, D.R.; Horne, D.A. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [CrossRef]
13. Dienlin, T.; Metzger, M.J. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *J. Comput. Mediat. Commun.* **2016**, *21*, 368–383. [CrossRef]
14. Min, J.; Kim, B. A study on continued intention of social network services by applying privacy calculus model: Facebook and KakaoTalk cases. *Inf. Syst. Rev.* **2013**, *15*, 105–122.
15. Dinev, T.; Hart, P. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [CrossRef]
16. Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *Eur. J. Inf. Syst.* **2013**, *22*, 295–316. [CrossRef]
17. Xu, H.; Teo, H.H.; Tan, B.C.Y.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manag. Inf. Syst.* **2010**, *26*, 135–173. [CrossRef]
18. Kim, B.; Min, J. The distinct roles of dedication-based and constraint-based mechanisms in social networking sites. *Internet Res.* **2015**, *25*, 30–51. [CrossRef]
19. Mosteller, J.; Poddar, A. To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *J. Interact. Mark.* **2017**, *39*, 27–38. [CrossRef]
20. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
21. Leem, J.M.; Rha, J.Y. Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Comput. Hum. Behav.* **2016**, *63*, 453–462.
22. Benson, V.; Saridakis, G.; Tennakoon, H. Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Inf. Technol. People* **2015**, *28*, 426–441. [CrossRef]
23. Phelps, J.; Nowak, G.; Ferrell, E. Privacy concerns and consumer willingness to provide personal information. *J. Public Policy Mark.* **2000**, *19*, 27–41. [CrossRef]
24. Zhoi, T.; Li, H. Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Comput. Hum. Behav.* **2014**, *37*, 283–289. [CrossRef]
25. Cheung, C.M.; Chiu, P.Y.; Lee, M.K. Online social networks: Why do students use Facebook? *Comput. Hum. Behav.* **2011**, *27*, 1337–1343. [CrossRef]
26. Li, F. Chinese tourists' barriers to sharing travel photos in WeChat. *Sustainability* **2020**, *12*, 887. [CrossRef]
27. Homans, C.G. *Social Behavior: Its Elementary Forms*; Harcourt, Brace & World: New York, NY, USA, 1961.
28. Laufer, R.S.; Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *J. Soc. Issues* **1977**, *33*, 22–42. [CrossRef]
29. Xu, H.; Gupta, S. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electron. Mark.* **2009**, *19*, 137–149. [CrossRef]
30. Westin, A.F. Social and political dimensions of privacy. *J. Soc. Issues* **2003**, *59*, 431–453. [CrossRef]
31. Kim, B. A study of antecedents of continuance intention in mobile social network service: The role of trust and privacy concerns. *Knowl. Manag. Res.* **2012**, *13*, 83–100.
32. Frampton, B.D.; Child, J.T. Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Comput. Hum. Behav.* **2013**, *29*, 2257–2264. [CrossRef]
33. Wu, P.F. The privacy paradox in the context of online social networking: A self-identity perspective. *J. Assoc. Inf. Sci. Technol.* **2019**, *70*, 207–217. [CrossRef]
34. Kroll, T.; Stieglitz, S. Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behav. Inf. Technol.* **2019**. [CrossRef]
35. Americans' Complicated Feelings about Social Media in an Era of Privacy Concerns. Available online: https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ (accessed on 24 June 2020).
36. Kobsa, A.; Patil, S.; Meyer, B. Privacy in instant messaging: An impression management model. *Behav. Inf. Technol.* **2012**, *21*, 355–370. [CrossRef]
37. Teubner, T.; Flath, C.M. Privacy in the sharing economy. *J. Assoc. Inf. Syst.* **2019**, *20*, 213–242. [CrossRef]
38. Fishbein, M.; Ajzen, I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*; Addison-Wesley: Boston, MA, USA, 1975.

39. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
40. Kim, B. Understanding the role of conscious and automatic mechanisms in social networking services: A longitudinal study. *Int. J. Hum. Comput. Interact.* **2018**, *34*, 805–818. [CrossRef]
41. Katz, E.; Blumler, J.G.; Gurevitch, M. Uses and gratifications research. *Public Opin. Q.* **1973**, *37*, 509–523. [CrossRef]
42. Hossain, N.A.; Kim, M.; Jahan, N. Can "Liking" behavior lead to usage intention on Facebook? Uses and gratification theory perspective. *Sustainability* **2019**, *11*, 1166. [CrossRef]
43. Malik, A.; Dhir, A.; Nieminen, M. Uses and gratifications of digital photo sharing on Facebook. *Telem. Inform.* **2016**, *33*, 129–138. [CrossRef]
44. Stafford, T.F.; Stafford, M.R.; Schkade, L.L. Determining uses and gratifications for the Internet. *Decis. Sci.* **2004**, *35*, 259–288. [CrossRef]
45. Hew, K.F. Students' and teachers' use of Facebook. *Comput. Hum. Behav.* **2011**, *27*, 662–676. [CrossRef]
46. Ku, Y.C.; Chu, T.H.; Tseng, C.H. Gratifications for using CMC technologies: A comparison among SNS, IM, and e-mail. *Comput. Hum. Behav.* **2013**, *29*, 226–234. [CrossRef]
47. Huang, L.Y.; Hsiehm, Y.J.; Wu, Y.C.J. Gratifications and social network service usage: The mediating role of online experience. *Inf. Manag.* **2014**, *51*, 774–782. [CrossRef]
48. James, T.L.; Warkentin, M.; Collignon, S.E. A dual privacy decision model for online social networks. *Inf. Manag.* **2015**, *52*, 893–908. [CrossRef]
49. Ifinedo, P. Applying uses and gratifications theory and social influence processes to understand students' pervasive adoption of social networking sites: Perspectives from the Americas. *Int. J. Inf. Manag.* **2016**, *36*, 192–206. [CrossRef]
50. Dwyer, C.; Hiltz, S.; Passerini, K. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, CO, USA, 9–12 August 2007; pp. 725–1735.
51. Chang, S.E.; Liu, A.Y.; Shen, W.C. User trust in social networking services: A comparison of Facebook and LinkedIn. *Comput. Hum. Behav.* **2017**, *69*, 207–217. [CrossRef]
52. Rau, P.L.; Gao, Q.; Ding, Y. Relationship between the level of intimacy and lurking in online social network services. *Comput. Hum. Behav.* **2008**, *24*, 2757–2770. [CrossRef]
53. Wang, T.; Duong, T.D.; Chen, C.C. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *Int. J. Inf. Manag.* **2016**, *36*, 531–542. [CrossRef]
54. Shin, D.H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.* **2010**, *22*, 428–438. [CrossRef]
55. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inf. Syst. Res.* **2004**, *15*, 311–416. [CrossRef]
56. Chadwick, S.A. Communicating Trust in E-Commerce Interactions. *Manag. Commun. Q.* **2001**, *14*, 653–658. [CrossRef]
57. Venkatesh, V.; Brown, S.A. A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges. *MIS Q.* **2001**, *25*, 71–102. [CrossRef]
58. Kim, S.S.; Malhotra, N.K.; Narasimhan, S. Two competing perspectives on automatic use: A theoretical and empirical comparison. *Inf. Syst. Res.* **2005**, *16*, 418–432. [CrossRef]
59. Chin, W.W. The partial least squares approach to structural equation modeling. In *Modern Methods for Business Research*; Marcoulides, G.A., Ed.; Lawrence Erlbaum: Mahway, NJ, USA, 1998; pp. 295–336.
60. Hair, F.; Sarstedt, M.S.; Ringle, C.M.; Mena, J.A. An assessment of the use of partial least squares structural equation modeling in marketing research. *J. Acad. Mark. Sci.* **2012**, *40*, 414–433. [CrossRef]
61. Hair, J.; Anderson, R.; Tatham, R.B. *Multivariate Data Analysis*; Prentice Hall: Upper Saddle River, NJ, USA, 1998.
62. Fornell, C.; Larcker, D.F. Evaluating structural evaluation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
63. Heirman, W.; Walrave, M.; Ponnet, K. Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychol. Behav. Soc. Netw.* **2013**, *16*, 81–87. [CrossRef] [PubMed]

64. Ji, Y.G.; Hwangbo, H.; Yi, J.S.; Rau, P.L.P.; Fang, X.; Ling, C. The Influence of Cultural Differences on the Use of Social Network Services and the Formation of Social Capital. *Int. J. Hum. Comput. Interact.* **2010**, *26*, 1100–1121. [CrossRef]
65. Makri, K.; Schlegelmilch, B.B. Time orientation and engagement with social networking sites: A cross-cultural study in Austria, China and Uruguay. *J. Bus. Res.* **2017**, *80*, 155–163. [CrossRef]