Hindawi Human Behavior and Emerging Technologies Volume 2023, Article ID 2643683, 14 pages https://doi.org/10.1155/2023/2643683



# Research Article

# **Self-Disclosure on Professional Social Networking Sites: A Privacy Calculus Perspective**

Imairi Eitiveni, Achmad Nizar Hidayanto, Yuvitri Annisa Dwityafani, and Larastri Kumaralalita

<sup>1</sup>Faculty of Computer Science, University of Indonesia, Depok, Indonesia <sup>2</sup>School of Business and Management, Royal Holloway, University of London, London, UK

School of Dustiness and Management, Royal Holloway, Oliversity of Bollaon, Bollaon,

Correspondence should be addressed to Imairi Eitiveni; imairi@cs.ui.ac.id

Received 21 November 2022; Revised 11 May 2023; Accepted 30 June 2023; Published 22 July 2023

Academic Editor: Mirko Duradoni

Copyright © 2023 Imairi Eitiveni et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The prevalence of social networking sites (SNS) raises questions about what information is private and what is not. Some users willingly share information on the site expecting some benefits, but others may be reluctant to do so due to fear of losing control of the shared information. To better understand the delicate relationship between privacy, perceived benefits, and self-disclosure, this study examines the antecedents of self-disclosure behavior on professional SNS (i.e., LinkedIn). A model contextualizing privacy calculus theory combined with the trust factor was developed and evaluated using 661 quantitative data collected through a questionnaire. Then, the data was analyzed using covariance-based structural equation modeling method. The results show that perceived benefit (e.g., self-presentation, career advancement, professional network development, learning, and information exchange), privacy concerns, and perceived control are the factors that directly influence LinkedIn users to disclose personal information. These factors become significant predictors of self-disclosure behavior. Meanwhile, trust in LinkedIn members, perceived severity, and perceived likelihood indirectly influence self-disclosure through privacy concerns. Finally, perceived control directly influences trust in LinkedIn members and trust in the LinkedIn provider. The findings of this study help to understand SNS users' behavior, particularly self-disclosure behavior. SNS users can become more aware of the benefits and risks of their disclosure behavior, allowing them to make more informed decisions. These findings can also be helpful for SNS providers to improve product experience and strategy by effectively encouraging and facilitating self-disclosure practices.

## 1. Introduction

Social Networking Sites (SNS) have become an increasingly important means of communication. These computer-based interactive technologies facilitate the creating and sharing of thoughts, ideas, and information [1]. SNS offer several advantages such as self-expression, finding entertainment, and searching for information [2, 3]. One widely used SNS is LinkedIn, with 14 million users [4]. LinkedIn is an employment-oriented SNS for professionals, job seekers, companies, and students to meet, exchange ideas, learn, and find employment opportunities [5]. Users can disclose their professional information by creating a summary including work experience and educational background information on their profile page [6]. Generally, users per-

form self-disclosure in order to be found more efficiently by recruiters and to be recognized as experts in a field (defined as self-presentation). Similarly, LinkedIn is becoming a more important source of information for recruiters in the recruitment process because it allows them to reach a wider range of candidates [7]. A survey by Jobvite [8] found that 89% of recruiters use LinkedIn to recruit applicants. Recruiters can assess prospective employees' skills and personalities from related information on LinkedIn such as profile pages and posts [9]. The success of this practice depends on the amount of information available. Therefore, understanding users' self-disclosure behavior is critical for effectively encouraging users to do so.

However, there are risks associated with disclosing personal information, such as the misuse of private information

and identity theft [10]. The prevalence of privacy threats increases users' concerns regarding the security of personal information [2]. For example, employees may not want their current employers to know that they are open for work or applying for other jobs. This issue affects users' willingness to disclose professional and personal information. Additionally, the level of knowledge related to privacy can influence the inclination to disclose information. A study by Zlatolas et al. [11] found that user knowledge about privacy issues and user concerns negatively affects users' intention to self-disclose. Hence, users may choose to limit the reveal of their information [12].

Disclosure of personal information can occur in various contexts such as on SNS, e-commerce transactions, and mobile applications. Several previous studies have explored the concept of self-disclosure. For example, Dinev and Hart [10] examined transactions in e-commerce using the privacy calculus theory. Krasnova et al. [13] focused on selfdisclosure on social networks, also using the privacy calculus theory. Zhao et al. [14] investigated location disclosure on mobile applications, while Liu et al. [15] studied selfdisclosure behavior on a Chinese microblogging site using social exchange theory. Unlike entertainment-oriented social media (e.g., Facebook and Snapchat), to the best of our knowledge, no studies have investigated the complex and delicate set of privacy issues, perceived benefits, and trust factors and their effect on self-disclosure on professional SNS such as LinkedIn. The benefits and risks of self-disclosure on entertainment-oriented social media differ from those on professional social media. For instance, professional SNS aim to advance careers, while entertainment-oriented social media primarily provide enjoyment factors [16].

Furthermore, in certain Asian cultures, including Indonesia, modesty is highly valued, and self-promotion is often viewed as undesirable. This cultural perspective can influence professionals' reluctance to disclose their achievements or contributions [17]. However, self-disclosure plays a crucial role in shaping how others perceive individuals, directly impacting their opportunities and success. Therefore, it is important to investigate the factors that motivate Indonesians to engage in self-disclosure, in order to provide them with better support. This study is aimed at examining the factors that influence self-disclosure behavior on professional social networking sites, specifically LinkedIn, in Indonesia. The research question guiding this study is "What are the factors that influence self-disclosure behavior on professional social networking sites?"

A literature review was performed to develop an initial theoretical framework to address this question. Because self-disclosure has both benefits and risks to privacy, this study contextualizes privacy calculus (PC) theory to investigate privacy issues related to self-disclosure on LinkedIn. PC theory suggests that individuals always rationally weigh the potential benefits and risks of personal information disclosure. Hence, it is a suitable theoretical approach to investigate the specific risks and benefits influencing users to disclose personal information on LinkedIn. Furthermore, because revealing oneself on a social network requires trust, this study also considers an extension of the trust factor,

namely, individual acceptance of SNS's ability to protect personal information [18].

This study is organized as follows. Section 2 elaborates on previous studies and theories as the foundations of this study, followed by the proposed theoretical framework. Section 3 describes the research methodology, which was reported and discussed in Sections 4 and 5, respectively. Then, section 6 explains the implications of this study. Finally, the conclusion, limitations, and suggestions for future research are provided in Section 7.

### 2. Literature Review

2.1. Self-Disclosure in Social Networking Sites. SNS are site-based services for users to create public or semipublic profiles within a restricted system, make connections with other users, and view a list of other users' connections [19]. The rapid development of SNS has significantly affected communication and social interactions. On SNS, for example, users can perform self-disclosure by sharing information and opinions while developing a professional persona.

Self-disclosure is the act or process of disclosing information related to oneself to others [20]. Several motives drive self-disclosure on SNS. First, self-disclosure brings happiness when performed [21]. Second, self-disclosure can strengthen the bond in relationships and benefit psychological health [22]. Another motivation to disclose personal information is self-presentation. Users can control how they present themselves on SNS compared to those when interacting in person by setting the personality they want to show [23, 24]. Finally, users can use the information provided by self-disclosure to expand personal interests, such as building professional relationships and creating business opportunities [25].

One of the most popular professional SNS is LinkedIn. It was inaugurated in 2003. It has over 660 million users across 200 countries [5]. LinkedIn allows users to display personal and professional information and contacts. Users can also add a short description on their LinkedIn profile to improve their self-presentation. Furthermore, users can also search for information about other users and companies, connect with other users, and form groups with similar interests to exchange information and expand professional networks.

However, disclosing or sharing information on social networks requires trust in technology and other users. Trust is an individual's belief or confidence in something or someone influenced by subjective norms, risk, self-confidence, and security [26]. Users who trust technology are willing to rely on system functions to protect them from threats and troubles [24]. Due to its conflicting nature, it is important to examine the interplay between trust and self-disclosure to effectively promote self-disclosure.

2.2. Privacy Calculus Theory. Privacy calculus (PC) theory posits that individuals, groups, or institutions determine for themselves when, how, and to what extent information about them is communicated to others [27]. PC theory assumes that individuals consider the future impact (costs and benefits) of taking actions [28]. In the context of

privacy, costs are related to the risks of disclosing information. When individuals provide personal information, the individual is involved in analyzing benefits and risks [27]. According to PC Theory, self-disclosure occurs when the benefits of communicating the information outweigh the costs [10]. Therefore, this study considers two factors: privacy costs and perceived benefits. Privacy cost is the potential loss of information control when disclosing it [10]. It is measured by the user's concern about self-disclosure on LinkedIn.

Meanwhile, the perceived benefit factor is a utilitarian benefit that motivates users to perform self-disclosure, such as self-presentation, learning and exchanging information, career advancement, and developing a professional network [15]. Self-presentation is defined as an act of controlling information to influence the impression perceived by the audience about the particular user [29]. LinkedIn provides an information space that allows users to present themselves and build personal identities. According to Boyd and Ellison [19], self-presentation is the main element that motivates users to perform self-disclosure on SNS.

Additionally, individuals also use SNS to exchange views and discuss need-related issues [30]. Users can take advantage of the discussion group feature of SNS by adding relevant information and establishing relationships with other users with similar interests [31]. Furthermore, professional SNS such as LinkedIn makes it easier to search for jobs and manage careers [30]. Recruiters use SNS to carry out the recruitment process by looking at the information contained in user accounts [31]. This factor can motivate users to complete information on social media to make it easier to be found by recruiters [32]. Finally, individuals develop a professional network by building connections with other users on SNS [15]. Self-disclosure is a central concept in relationship development [33]. Self-disclosure is performed not only to establish but also to maintain relationships with a wide range of users [21].

2.3. Related Studies. Several theories have been utilized to understand self-disclosure, such as PC theory (e.g., [10, 13, 14, 34]), protection motivation theory (e.g., [35]), communication privacy management theory (e.g., [11]), and uses and gratification theory (e.g., [30, 31]). For instance, Dinev and Hart [10] used PC theory to investigate e-commerce transactions. Their findingsrevealed that privacy concerns have a negative effect on e-commerce transactions. However, trust in the Internet and personal interest can positively influence users' disclosure decisions. Similarly, Krasnova et al. [13] applied PC theory to study self-disclosure in SNS. The results indicate a significant effect between perceived enjoyment and privacy concerns on the amount of information disclosed. In addition, privacy concerns are determined by perceived likelihood and perceived damage.

Given the emphasis of PC Theory on the perceived benefits of self-disclosure on social media, it is essential to investigate the motivation to use social media platforms in the first place. Therefore, Grissa [30] conducted a study to investigate the motivation to use professional SNS. The results revealed that individuals are motivated to use professional

SNS for a variety of reasons including looking for work, building personal branding, highlighting user expertise, building specific professional networks, and obtaining and exchanging information. Similarly, Florenthal [31] investigated students' motivations and barriers to using professional SNS, identifying motivations such as building a professional network, self-presentation, obtaining information, and advancing one's career.

Disclosure of personal information can occur in various contexts, such as on SNS, e-commerce transactions, and mobile applications. Wang et al. [35] studied users' intentions to disclose personal information on mobile applications. Their study found that self-presentation and service personalization factors positively affect users' intentions to disclose personal information, with perceived benefit factors as the mediating variable. Perceived severity and perceived control function as direct antecedents of perceived risk, which negatively impact users' intentions to disclose personal information. The results show that mobile application users consider the benefits of using mobile applications more than the risks, so users enter personal information willingly.

The geographical context seems to influence self-disclosure behavior. Krasnova and Veltri [36] surveyed Facebook users in Germany and USA to explore their cultural differences in self-disclosure on social media. The results indicate that Americans experience more perceived benefits in using Facebook, more perceived control over shared information, and more trust in social media providers than their German users. On the other hand, Germans have higher expectations of privacy damage and breaches. Meanwhile, Liu et al. [15] investigated self-disclosure in Chinese microblogging using social exchange theory. Their study found that relationship building, enjoyment, and trust in service providers significantly influence self-disclosure. However, self-presentation factors do not affect self-disclosure, and perceived risk factors negatively affect self-disclosure.

Previous studies demonstrated that privacy concerns affect self-disclosure behavior. Zlatolas et al. [11] investigate the impact of privacy-related problems on self-disclosure in SNS. They surveyed 661 SNS users in Slovenia and found that privacy awareness, privacy social norms, privacy policy, privacy values, and privacy concerns significantly affect self-disclosure. Finally, Zhao et al. [14] explored factors affecting the disclosure intention of location-related information on location-based SNS. Their findings show a significant influence between privacy concerns, personalization, and connectedness on the intention to disclose information. Specifically, privacy control has a negative effect on privacy concerns. Table 1 shows a summary of the previous studies examined in this study.

# 3. Research Model and Hypotheses

This study analyzes factors influencing users to self-disclose on professional SNS (i.e., LinkedIn) using PC theory, trust, and perceived control factors. PC theory was employed to explore users' perceptions when conducting self-disclosure. It examines the specific risks and benefits influencing users to disclose personal information on professional SNS. Thus,

Paper	Context	Theory	Methodology	Key findings
Dinev and Hart [10]	E-commerce transaction	PC theory	Survey	Factors influencing self-disclosure are perceived internet privacy risk, internet privacy concerns, internet trust, personal internet interest, willingness to provide personal information
Kranova and Veltri [36]	SNS usage in Germany and USA	PC theory	Survey	Factors influencing self-disclosure are benefits (e.g., enjoyment, self-presentation, relationship maintenance), privacy costs (e.g., privacy concerns, perceived likelihood, perceived damage), trust in SNS members, trust in SNS providers, perceived control, awareness, and trust in legal assurance
Krasnova et al. [13]	Online social network	PC theory	Survey	Factors influencing self-disclosure are trust in other OSN members, trust in OSN providers, perceived control, perceived privacy, risk, convenience, relationship building, self-presentation, and enjoyment.
Wang et al. [35]	Mobile applications	Protection motivation theory	Survey	Factors influencing self-disclosure are perceived benefits (e.g., personalized service, self-presentation), perceived risks (e.g., perceived severity, perceived control)
Zlatolas et al. [11]	Social media (i.e., Facebook) in Slovenia	Communication privacy management theory	Survey	Factors influencing self-disclosure are privacy awareness, privacy social norms, privacy policy, privacy value, privacy concern, privacy control
Grissa [30]	Professional networking sites	Uses and gratifications theory	Interviews and focus groups	Personal motivations for using professional networking sites are job seeking, career management, personal branding, developing a professional network, dan learning and exchanging information
Florenthal [31]	Professional networking sites	Uses and gratifications theory	Survey and interviews	Students' motivations for using LinkedIn are interpersonal communication, online identity, information, and career advancement

TABLE 1: Summary of the previous studies.

it is suitable for answering the research question of this study. Additionally, because disclosing oneself to a social network requires trust, this study also uses an extension of the trust factor, namely, individual acceptance of the ability of SNS to protect personal information [18]. Finally, since self-disclosure has also resulted from perceived control over information setting and dissemination, the perceived control factor is also included. The theoretical framework proposed in this study is presented in Figure 1, while the causality relationship of the variables in the theoretical framework is explained as follows.

A perceived benefit is the advantage that users expect to gain from disclosing their information on SNS. The greater users' perceived benefits, the more likely they are to self-disclose [37]. SNS users have several motivations for disclosing their personal information, such as self-presentation, learning and exchanging information, career advancement, and developing a professional network [30, 31].

Social networks can be used for professional purposes such as personal branding, self-promotion, and impression management [15, 38, 39] or broadly defined as self-presentation. Self-presentation is defined as an information-controlling activity aiming at influencing the impression formed by the audience about the user [29]. Self-presentation allows users to set the personality they want to present by selecting the types of information they wish to disclose [24]. For example,

users can use SNS to display education, work experience, skills, achievements, qualifications, descriptions related to users' social life, and public speech. Hence, when compared to direct interactions, users experience more control over their self-presentation on SNS [23]. This increased sense of control may encourage them to disclose more information on SNS. Thus, the authors hypothesize the following:

H1: self-presentation affects LinkedIn users' self-disclosure behavior of LinkedIn users.

Additionally, individuals use SNS to learn and discuss issues related to needs and interests [30]. With LinkedIn, searching for information and articles related to the target companies can make it easier for users to fully understand the organization. In addition, users can take advantage of the discussion group feature on LinkedIn. Users can add information according to the needs of other users, which can trigger a discussion with those with similar interests. This feature can encourage users to complete personal information relevant to the user's professional network [31]. Thus, the authors hypothesize the following:

H2: learning and exchanging information affect the selfdisclosure behavior of LinkedIn users.

SNS makes it easier to search for jobs and manage careers by searching for relevant jobs [30]. Users often use LinkedIn to find information about a person or a company and look for job information. Correspondingly, recruiters

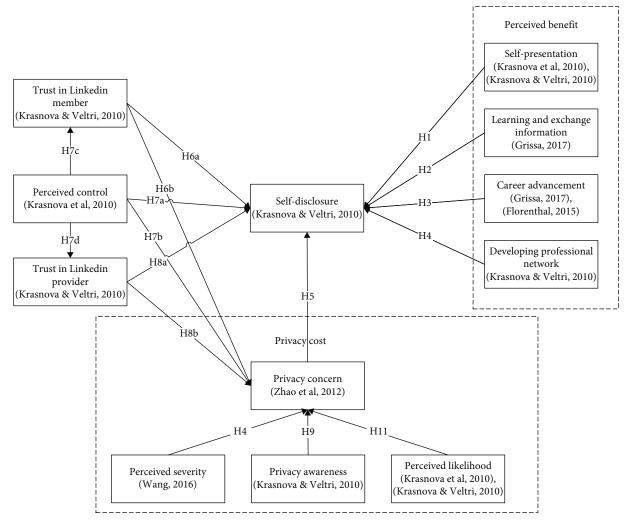


FIGURE 1: The initial research model.

use social media to conduct the recruitment process by looking at the information provided in user accounts [31]. Recruiters can assess prospective employees' skills and personalities from the information available on LinkedIn [9]. Since recruiters rely on publicly available information in recruitment selection, the lack of information provided by SNS may hinder career advancement [32]. These factors can motivate users to complete information on social media to make it easier to find suitable jobs and to be found by recruiters. Hence, the authors propose the following:

H3: career advancement affects the self-disclosure behavior of LinkedIn users.

Developing professional networks is defined as users who build connections with other users through SNS [15]. SNS make it easier for users to create professional business networks with a wide range of users. Self-disclosure is fundamental to achieving that goal since self-disclosure is crucial in relationship development [33]. Users can use the information provided by other users to build professional relationships and create business opportunities [25]. Incomplete relevant information on LinkedIn reduces the chance that the user is found by other users [15]. Furthermore,

self-disclosure is not only for establishing relationships but also for maintaining them [21]. Thus, the authors hypothesize the following:

H4: developing a professional network affects the self-disclosure behavior of LinkedIn users.

Previous studies state that privacy concerns affect information disclosure behavior [10, 40]. Privacy concern is the level of users' consideration about the flow, transfer, and exchange of their personal information [41]. The higher the privacy concern, the lower the user's intention to self-disclosure. Furthermore, Krasnova et al. [34] found that privacy concern also affects the amount of information provided on SNS. High privacy concerns may cause minimal information provided on the platform. Thus, the authors propose the following:

H5: privacy concern affects the self-disclosure behavior of LinkedIn users.

Trust in a communication channel and its members is crucial for predicting self-disclosure behavior. Trust can reduce the privacy costs of disclosing personal information [42, 43]. SNS produce virtual intimacy and perceived similarities which can induce trust among its members. Hence,

users perceive fewer risks in providing personal information on the platform. If users believe that others will not misuse the information provided, they are more likely to disclose their personal information [13]. Thus, the authors propose the following:

H6a: trust in LinkedIn members affects the self-disclosure behavior of LinkedIn users.

Trust in other LinkedIn users also affects privacy concerns. The lack of ability to directly monitor other members' use of the information provided reflects implicit trust in others. Joinson and Paine [44] argue that users tend to idealize their fellow SNS members. This individual belief regarding other members' trustworthiness may affect privacy concerns. If users believe that other members will not misuse the information provided, it will reduce their level of concern [13]. Hence, the authors hypothesize the following:

H6b: trust in LinkedIn members affects the privacy concerns of LinkedIn users.

Trust in SNS service providers is essential to determine the possibility of users disclosing personal information [16]. This trust can be affected by the service provider's integrity, transparency, and security. If the users perceive that the SNS service provider can be trusted, the privacy costs will decrease, and the benefits will increase [16]. Liu et al. [15] found that when SNS users know that SNS pays attention to security, users will trust the service and share information with the site [15]. To gain trust and encourage complete information disclosure from users, SNS need to implement information privacy guarantees [45]. Thus, the authors hypothesize the following:

H8a: trust in LinkedIn providers affects the self-disclosure behavior of LinkedIn users.

Additionally, trust in SNS service providers affects privacy concerns. Similarly, the service provider's integrity, transparency, and security reduce perceived privacy costs [16]. Pavlou [46] emphasized the importance of trust in mitigating privacy risks. Furthermore, [47] highlighted that trust in the SNS provider reduces privacy concerns when sharing information on the platform. Thus, we hypothesize the following:

H8b: trust in LinkedIn providers affects the privacy concerns of LinkedIn users.

The level of control over access to their information affects users' self-disclosure behavior. The privacy control factor measures how much users can control access to their personal information [11]. LinkedIn provides features that control access to information. For example, users can set what information can be displayed on their profile. Since users can control who can view their information on SNS, the presence of privacy settings may encourage users to disclose information [48] since users can control who can view their information on the SNS. Thus, the authors propose the following hypothesis:

H7a: perceived control affects the self-disclosure behavior of LinkedIn users.

Perceived control also affects users' concerns over information sharing on SNS. The existence of privacy settings on LinkedIn can reduce users' privacy concerns [48]. Jozani

et al. [49] found that even if users have limited control over their personal information if the service provider explicitly requests permission to access it, users feel they can exercise control and reduce privacy concerns. Thus, the authors propose the following:

H7b: perceived control affects the privacy concerns of LinkedIn users.

Perceived control is related to users' ability to control personal information on social media [11]. LinkedIn provides features that control access to information, such as setting what information can be displayed. The settings create the perception that users can control the information on SNS [16]. SNS users tend to trust other users when they can manage their privacy, such as by limiting access to profiles, comments, and posts on SNS [13]. Thus, the authors hypothesize the following:

H7c: perceived control affects trust in LinkedIn members. Additionally, perceived control also affects trust in the LinkedIn provider. If users believe that they control their information via privacy settings on the SNS platform, it increases trust in SNS service providers, eventually encouraging self-disclosure [13]. Hence, the authors propose the following:

H7d: perceived control influences users' trust in the LinkedIn service provider.

Privacy awareness is the degree to which users know about privacy practices on SNS [11]. Users with a high level of privacy awareness consider privacy issues on SNS sites, which then influences their behavior. According to Boyd and Ellison [19], users are becoming more concerned about privacy issues on SNS, such as unintentional and harmful privacy losses. This awareness affects the level of user concern when disclosing personal information. Thus, the authors propose the following:

H9: privacy awareness affects privacy concerns in LinkedIn users.

Previous studies revealed that perceived severity influences privacy concerns [35, 50]. Perceived severity indicates an attitude in which users perceive negative consequences caused by security threats. Then, this perception triggers privacy protection behavior. Perceived severity is closely related to protective and avoidance behavior [35]. Users with a high level of perceived severity tend to have serious concerns about information security and take action to protect their personal information [35, 50]. Accordingly, the authors propose the following:

H10: perceived severity affects privacy concerns in LinkedIn users.

Finally, previous studies showed that perceived likelihood influences privacy concerns [35, 50]. The perceived likelihood is the possibility of a negative outcome when disclosing information on social media. Like perceived severity, the perceived likelihood also triggers privacy protection behavior. A high level of perceived likelihood tends to cause serious concerns about information security and lead to information concealment [35, 50]. Thereupon, the authors propose the following:

H11: perceived likelihood affects privacy concerns of LinkedIn users.

# 4. Research Methodology

4.1. Respondents. This study used a quantitative approach to validate the proposed theoretical framework. The approach aims to identify the relationship between the independent and dependent variables in one population [51]. Since this study investigates factors influencing self-disclosure behavior on LinkedIn, data for this study were collected through a survey of active users of LinkedIn. The survey was distributed to various social media platforms such as Twitter, LinkedIn, Instagram, and Line because these platforms are used by most social media users in Indonesia.

4.2. Measurements. In total, eleven variables were included in this study: self-presentation (SP), learning and exchange information (LEI), career advancement (CA), developing professional network (DP), privacy concern (PC), perceived severity (PS), privacy awareness (PA), perceived likelihood (PL), trust in LinkedIn members (TM), trust in LinkedIn provider (TP), and perceived control (CON). The research instrument consisted of two parts. The first section contains questions regarding users' demographics (e.g., gender, age, education, and occupation) and their experience with using LinkedIn. The second part of the questionnaire consists of statements to be assessed by the respondents based on their experiences and observations when using LinkedIn. The measurement items for each variable are provided in Appendix A. The assessment used a 5-point Likert scale varying from 1 (strongly disagree) to 5 (strongly agree). The questionnaire was reviewed by ten respondents to clarify the statements. Based on the review results, the questionnaire was revised and then distributed.

4.3. Data Analysis. In conducting data analysis, the authors used the covariance-based structural equation modeling (CB-SEM) technique using AMOS 24.0 software. SEM is a statistical model technique that measures the relationship between variables by testing the structure of the model. The CB-SEM technique uses the covariance matrix of the data and estimates model parameters by considering the general variance, while the PLS-SEM is variance-based and uses the total variance to estimate parameters [52]. CB-SEM involves a maximum likelihood procedure that aims to reduce the difference between the observed covariance matrix and the tested covariance matrix. In research using the CB-SEM technique, it is necessary to assume that the data is normally distributed. This study performed measurement model testing and structural model testing to measure the proposed model.

# 5. Data Analysis and Results

The data collection took four weeks and yielded 935 records. However, 274 data points were incomplete and, hence, were not included in the analysis. The remaining 661 data were complete and valid. According to Hair Jr., et al. [53], research using CB-SEM should have 5-10 data for each indicator. Since this study has 36 indicators, the minimum data requirement is fulfilled.

5.1. Demography. Of 661 respondents, 240 were male (36.3%), and 421 were female (63.7%). Most respondents (393) were between the age of 17 and 22. People with bachelor's degrees dominate the respondents in terms of education. Meanwhile, most respondents are private-sector employees who have used LinkedIn for 1 and 2 years, mainly for job searching. More detailed demographic data can be seen in Table 2.

5.2. Measurement Model Testing. Several assumptions and conditions must be fulfilled before conducting a measurement model, i.e., degree of freedom (DoF), normally distributed data, data completeness, outliers, and multicollinearity. Data analysis showed the DoF value of the proposed research model is 528. Since it is positive, the model is said to be overidentified. Hence, model assessment can be performed [54]. Based on the data normality test, this study has a composite reliability (CR) value of 39.628, which falls outside the range of normally distributed multivariate data (c.r. value between -2.58 and +2.58) [54]. Hence, it is necessary to remove outliers. Data classified as outliers are those with p1 and p2 values at the Mahalanobis distance < 0.001 [54]. Based on this value, 30 data were deleted. Then, the multivariate normality of the CR value for the overall data was recomputed, which produced a value of 34.947. Based on these results, a bootstrapping approach was taken to normally distribute the data. Then, a multicollinearity test was performed to ensure that each indicator represents a different aspect, so the correlation between indicators is expected to be low. The results showed no correlation between the indicators with a value of  $\geq$  0.9, which means there is no multicollinearity in the data [54].

Reliability and validity testing measures whether the indicators can explain the constructs in the research model by examining the loading factor, composite reliability (CR), Cronbach's alpha (CA), and average variance extracted (AVE) values [54].

The acceptable thresholds for factor loading value and CR are both 0.7. Meanwhile, the AVE value for each construct must exceed 0.5 to pass the testing. CA values above 0.5 show moderate to high reliability [55]. Data analysis showed that after six iterations, PA3, CON3, PL3, PS1, TP1, and SD1 had loading factor values less than 0.7, meaning that they have relatively little influence on the measured variables [52]. Hence, they were deleted. The results showed that the values of CA, AVE, and CR for all constructs have been met, which means that the result of this study is reliable and valid, as shown in Table 3.

Then, a discriminant validity test was performed by calculating the square root of AVE. If the value is greater than the existing correlation value, it passes the discriminant validity test [54]. The test results showed that all AVE root values are greater than the correlation value with other variables, as shown in Table 4. Hence, it can be concluded that the proposed research model passed the discriminant validity test.

Next, the measurement model was subjected to a goodness of fit test. As shown in Table 5, the result demonstrated the overall goodness of fit was met for all indicators and the

TABLE 2: Respondent demographics.

Respondents' demograp	Amount	Percentage	
Gender	Female	421	36.3
Gender	Male	240	63.7
	<17	2	0.3
	17-22	393	59.5
A ~~	23-28	224	33.9
Age	29-34	33	5
	35-40	7	1.1
	>41	2	0.3
	Junior high school	1	0.2
	High school	57	8.6
Education	Diploma	34	5.1
Education	Bachelor's degree	530	80.2
	Master's degree	37	5.6
	Doctorate degree	2	0.3
	Student	285	43.1
	Civil servant	15	2.3
	State-owned		
	enterprise	9	1.4
Occupation	employee		
Cecupation	Private sector employee	203	30.7
	Entrepreneur	25	3.8
	Unemployed	98	14.8
	Others	26	3.9
	<1 year	153	23.1
	1 and 2 years	263	39.8
LinkedIn use duration	3-5 years	215	32.5
	6-10 years	25	3.8
	>10 years	5	0.8
		90	13.6
	Updating personal information	308	46.6
	mormation	127	19.2
	Job searching	24	3.6
Activities on LinkedIn	Learning	109	16.5
	Updating self with others' info	3	0.5
	Building connection		
	Sharing experience		
	Identity theft	20	3
Privacy issues	Scam	45	6.8
experienced on LinkedIn	No problem	588	89
LIIIKCUIII	Others	8	1.2

measurement model, which means that the structural model fitted the research model. The causal relationship within the model was demonstrated; hence, it did not required modification.

5.3. Structural Model Testing. For structural model testing, hypothesis testing using a two-tailed test at a significance level of 5% output was conducted. Table 6 shows five rejected hypotheses and 11 accepted hypotheses. Therefore, the research model was modified. The final research model is shown in Figure 2.

#### 6. Discussion

This study is aimed at determining the factors influencing user intention to disclose personal information on SNS (i.e., LinkedIn). The results show that the perceived benefits of self-disclosure on SNS, such as self-presentation, learning and exchanging information, career advancement, and developing a professional network, positively influence selfdisclosure behavior on LinkedIn. This finding is consistent with the findings of Emad ALQadheeb and Ibraheem Alsalloum [16], who found several perceived benefits of self-disclosure on networking sites, including self-presentation, the ease of maintaining existing relationships, and the convenience of building new relationships. Additionally, SNS users also benefit from newly found information and interaction with others [16]. SNS, such as LinkedIn, make it easy for individuals to build connections and maintain relationships with various companies and backgrounds [56]. Finally, the most significant perceived benefit factor when conducting self-disclosure on LinkedIn is career development. This result is in line with the goal of LinkedIn, which is to accelerate one's career.

The findings also show a significant relationship between perceived control and information disclosure behavior on LinkedIn. LinkedIn allows users to manage the information displayed and limit who can view it. This perceived control boosts users' trust in the SNS, influencing the actual disclosure of personal information [11, 57].

On the contrary, privacy concern negatively affects self-disclosure behavior. This finding is in line with [11, 58], who showed that a high level of uncertainty about who can view and potentially abuse the information published on SNS increases users' apprehension. This concern affects the amount of information disclosed. If users are highly concerned about the possibility of privacy breaches when disclosing personal information, the amount of information disclosed to SNS will be significantly reduced.

Furthermore, privacy concern itself is influenced by perceived likelihood, perceived severity, and trust in LinkedIn members. This result corresponds to Krasnova et al. [13], who found that perceived likelihood strongly influences privacy concerns. Individual assessment of negative probabilities is often distorted because of an optimistic bias that worries users about the risks involved. Similarly, Wang et al. [35] found that perceived severity is highly related to protective and avoidance behaviors. Individuals who perceive significant consequences of losing personal information when disclosing information tend to be more concerned about information security and will protect their information. Finally, trust in other users can affect self-disclosure behavior through privacy concerns. This finding is consistent with the findings of [16], who found that if SNS users trust other users

TABLE 3: The result of the measurement model test.

Variable	Indicator	Loading factor	CR	CA	AVE	Variable	Indicator	Loading factor	CR	CA	AVE
	PC1	0.738			0.809	Developing professional	DP1	0.777			
Privacy concern	PC2	0.866	0.849 0.845	0.845			DP2	0.863	0.864	0.863	0.825
	PC3	0.816				network	DP3	0.833			
	PA1	0.768		0.732	0.764	Self-presentation	SP1	0.794			
Privacy awareness	PA2	0.74	0.737				SP2	0.888	0.889	0.886	0.853
	PA3	0.516					SP3	0.875			
	CON1	0.734	0.751		17 0.776	Trust in LinkedIn provider	TP1	0.582			
Perceived control	CON2	0.807		0.747			TP2	0.817	0.728	0.726	0.757
	CON3	0.605					TP3	0.702			
	PL1	0.863	0.835	0.83	0.847	Self-disclosure	SD1	0.619			
Perceived likelihood	PL2	0.817					SD2	0.784	0.71	0.706	0.742
	PL3	0.636					SD3	0.729			
	PS1	0.631			0.821		CA1	0.775			
Perceived severity	PS2	0.795	0.806	0.805		Career advancement	CA2	0.75	0.853	0.836	0.793
	PS3	0.841				advancement	CA3	0.849			
Learning and exchange information	LEI1	0.844					TM1	0.874			
	LEI2 0.919 0.8	0.894	0.892	0.86	Trust in LinkedIn members	TM2	0.88	0.863	0.857	0.825	
	LEI3	0.812				members	TM3	0.708			

Table 4: Comparison of AVE values with intervariable correlation.

	PC	PA	CON	PL	PS	LEI	DP	SP	TP	SD	CA	TM
PC	0.809											
PA	0.178	0.764										
CON	0.189	0.664	0.776									
PL	0.698	0.143	0.122	0.847								
PS	0.554	0.287	0.389	0.374	0.821							
LEI	0.065	-0.055	0.004	0.017	-0.025	0.86						
DP	0.188	0.439	0.47	0.126	0.337	-0.041	0.825					
SP	0.266	0.472	0.581	0.222	0.491	-0.012	0.709	0.853				
TP	0.061	0.713	0.606	-0.009	0.24	0.003	0.371	0.439	0.757			
SD	0.218	0.41	0.529	0.206	0.459	-0.115	0.58	0.663	0.433	0.742		
CA	0.241	0.48	0.491	0.214	0.413	-0.016	0.662	0.753	0.455	0.67	0.793	
TM	-0.085	0.531	0.401	-0.112	0.035	-0.04	0.165	0.181	0.673	0.214	0.152	0.825

to be trustworthy and not misuse information, the user perceives a lower level of privacy risk, which influences information disclosure behavior.

Nonetheless, the results show that privacy concern is not influenced by privacy awareness, trust in the LinkedIn provider, and perceived control. This study suspected that the reason for its rejection is that Indonesians enjoy the perceived benefits of self-disclosure regarding privacy risks, as 54% of respondents revealed that they are unaware of the privacy risks of disclosing their personal information. This finding contradicts Zlatolas et al. [11], who state that the higher the level of knowledge about privacy, the higher the level of user concerns. Similarly, there is no significant relationship between trust in LinkedIn providers with privacy

concerns. This result could be explained by the fact that LinkedIn users in Indonesia may not have a high level of trust in LinkedIn services, so there is no significant relationship between the level of user concern and the level of user trust. Additionally, there is no significant relationship between perceived control and privacy concerns. This result could be explained by the possibility that LinkedIn users' confidence in privacy settings cannot alleviate their concerns when disclosing information to LinkedIn. This possibility is in line with Mukaromah et al. [59], who assert that user-perceived control does not affect risk. On the contrary, Zlatolas et al. [11] contend that when users believe they have reasonable control over privacy settings in SNS, they will pay more attention to privacy.

Measurement criteria	Cut-off value	Result	Remarks
Chi-Square	>0.05	465.358	Good fit
CMIN/df	≤2	1.373	Good fit
CMIN	CMIN saturated model < CMIN default model <cmin independence="" model<="" td=""><td>Saturated model: 0.00 Default model: 465.358 Independence model: 10460.796</td><td>Good fit</td></cmin>	Saturated model: 0.00 Default model: 465.358 Independence model: 10460.796	Good fit
GFI	>0.9	0,954	Good fit
RMR	Close to 0	0.019	Good fit
CFI	>0.9	0.987	Good fit
NFI	>0.9	0.956	Good fit
TLI	>0.9	0.984	Good fit
RMSEA	< 0.05	0.024	Good fit

TABLE 5: The result of goodness of fit test.

TABLE 6: Hypothesis testing results.

Hypothesis	Result	Hypothesis	Result
H1: self-presentation affects self-disclosure behavior	Supported	H7a: Perceived control affects self-disclosure behavior	Supported
H2: learning and exchanging information affect self-disclosure behavior	Supported	H7b: Perceived control affects privacy concern	Nonsupported
H3: career advancement affects self-disclosure behavior	Supported	H8a: Trust in LinkedIn providers affects self-disclosure behavior	Nonsupported
H4: developing a professional network affects self-disclosure behavior	Supported	H8b: Trust in LinkedIn providers affects privacy concern	Nonsupported
H5: privacy concern affects self-disclosure behavior	Supported	H9: Privacy awareness affects privacy concern	Nonsupported
H6a: trust in LinkedIn members affects self-disclosure behavior	Nonsupported	H10: Perceived severity affects privacy concern	Supported
H6b: trust in LinkedIn members affects privacy concern	Supported	H11: Perceived likelihood affects privacy concern	Supported

Next, data analysis shows no significant relationship between trust in LinkedIn members and providers with self-disclosure behavior. This finding contradicts Krasnova et al. [13], who found that there is a substantial relationship between trust in SNS members and providers with self-disclosure behavior. However, this study's finding is in line with Ningroem et al. [60], who showed that respondents' trust in information providers and fellow users on Facebook does not affect their willingness to upload personal information.

Finally, the findings show a significant relationship between perceived control and users' trust in the provider services and other users. This result is in line with Emad ALQadheeb and Ibraheem Alsalloum [16], who found that SNS services allow users to control privacy settings that affect the trust in the SNS service providers and users. By exercising control over access to personal information, users can regulate what information can be accessed by other users. For example, LinkedIn users can limit the information displayed before adding other users.

# 7. Implications

This study contributes to the literature by identifying factors influencing users to disclose information on LinkedIn.

Currently, most research related to self-disclosure discusses general SNS from different perspectives (e.g., entertainment and financial transactions). The model from the study contributes new knowledge concerning the antecedents of self-disclosure behavior in SNS. Additionally, this study explores self-disclosure practices in a developing country, which may raise new perspectives due to its uniqueness and cultural conditions. Generally, in Indonesia, self-disclosure or personal branding may cause discomfort for the actor or people around them since humility and modesty are still more culturally valued. This study fills the gap in the literature by exploring how Indonesians reconcile their values with self-disclosure in professional SNS.

From a practical perspective, this study's findings can be helpful to professional SNS providers in understanding the factors that influence self-disclosure behavior. As a result, service providers can add and improve features that encourage and facilitate self-disclosure. The results of this study can be used as a reference to develop features that consider the benefits and risks perceived by users when disclosing personal information. For example, as one of the perceived benefits of self-disclosure behavior is learning and exchanging information, service providers can add features such as a tag feature that helps users to find relevant articles. Additionally, since

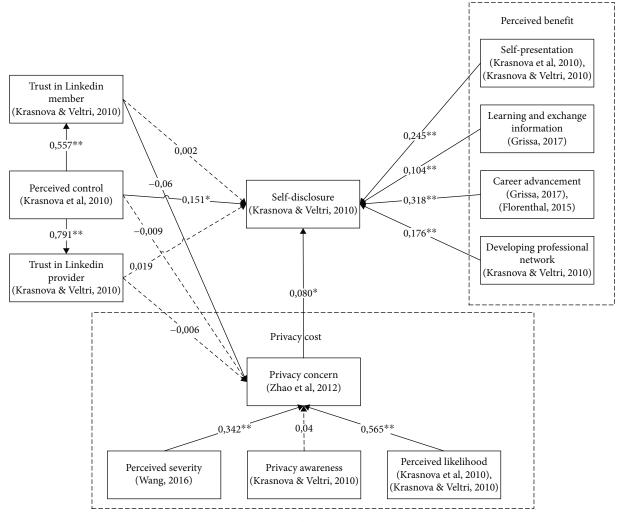


FIGURE 2: The final research model.

information control affects self-disclosure, service providers can enable users to manage information access. Since there is a relationship between information control with self-disclosure, service providers can provide features to manage information access. Furthermore, service providers can explain to users about privacy practices and risk mitigation provided by service providers, reducing the level of concern about the possibility of information misuse when disclosing personal information.

#### 8. Conclusion

This study is aimed at determining factors influencing the willingness to disclose personal information on professional SNS with LinkedIn as the case study. Data were collected using questionnaires to LinkedIn users, which were then analyzed using the CB-SEM method in AMOS 24.0. The main findings of this study are as follows.

First, this study identified the factors that significantly influence personal information disclosure behavior are perceived benefits, privacy concerns, and perceived control. The perceived benefits include self-presentation, career advancement, professional network development, and learning and

information exchange. Second, the results of this study revealed factors that significantly influence user concerns when disclosing professional information to LinkedIn are perceived likelihood, perceived severity, and trust in LinkedIn members. Third, the results show that perceived control significantly influences users' trust in other users and LinkedIn services.

This study has several limitations. First, despite our best efforts to identify and examine the significant and relevant variables, data analysis shows that the trust factor in other LinkedIn members is 0.312. This means that there are still unexplored factors associated with trust. Future studies may add other factors that influence self-disclosure behavior. Future research may also investigate factors that influence self-disclosure behavior from various factors other than users' perspectives, such as user management services, social aspects, and user environmental aspects. Second, the majority of respondents in this study were between the ages of 17 and 22. Because age influences the level of privacy awareness on social media, the findings could be limited to this age group. The authors, however, advise SNS developers to provide appropriate services and features for this category.

Third, the respondents examined in this study are limited to Indonesian LinkedIn users. Comparison with other countries regarding their self-disclosure behavior may benefit future research. Finally, this is a quantitative study using a survey to collect data. Further explanation about the findings may arise from other methodological designs such as a qualitative perspective using interviews and observations.

# **Appendix**

#### Measurement Items

Self-presentation (adapted from Krasnova and Veltri [36] and Krasnova et al. [13])

- (1) LinkedIn allows me to make a good impression professionally
- (2) LinkedIn allows me to represent myself professionally
- (3) LinkedIn helps me to show my best side to others in a professional manner

Learning and exchange information (adapted from Grissa [30])

- (1) I share and seek information from other LinkedIn users
- (2) I discuss and exchange work experiences with other LinkedIn users
- (3) I join or participate in groups related to my needs

Career advancement (adapted from Grissa [30] and Florenthal [31])

- (1) I believe LinkedIn can help me to get a job
- (2) I feel that LinkedIn is a social media for finding jobs
- (3) LinkedIn is useful for my career advancement

Developing professional network (adapted from Krasnova and Veltri [36])

- (1) LinkedIn really helps me in building relationships with professional workers
- (2) It is very easy to keep professional relationships using LinkedIn
- (3) LinkedIn is useful for developing business and personal relationships

Privacy concern (adapted from Zhao et al. [14])

- (1) I am concerned that a person can find private information about me on LinkedIn
- (2) I am concerned that the information I provide on LinkedIn would be abused by other parties

(3) I am concerned that the information I disclose on LinkedIn would cause unexpected problems

Perceived likelihood (adapted from Krasnova et al. [34] and Krasnova and Veltri [36])

- (1) The information I disclose on LinkedIn will be used by other users in unexpected ways
- (2) The information I provide on LinkedIn may be accessible to unwanted users
- (3) The information I submit to LinkedIn may be used with me

Perceived severity (adapted from Wang et al. [35])

- (1) I believe that losing information privacy through LinkedIn will be a serious problem for me
- (2) If my online identity is stolen by other users, then it becomes a serious problem for me
- (3) Losing personal information privacy via LinkedIn would be a critical issue for me

Privacy awareness (adapted from Krasnova and Veltri [36] and Zlatolas [11])

- (1) In general, I think LinkedIn is transparent about how it uses the personal information I provide
- (2) LinkedIn clearly states what data it collects from me
- (3) I am aware of the privacy concerns and procedures on LinkedIn

Trust in LinkedIn members (adapted from Krasnova and Veltri [36])

- (1) I am sure other LinkedIn users would not misuse the information they get from my LinkedIn profile or posts
- (2) I do not doubt that LinkedIn users will not use information about me in the wrong way
- (3) Generally, I believe LinkedIn users can be trusted

Trust in the LinkedIn provider (adapted from Krasnova and Veltri [36] and Dwyer et al. [47])

- (1) In my opinion, LinkedIn is responsible for the data that has been provided by users
- (2) I feel that LinkedIn can protect the privacy of my personal information
- (3) I trust LinkedIn will not use my information for any other purpose

Perceived control (adapted from Krasnova et al. [13])

(1) I can control the information I submit to LinkedIn

- (2) The privacy settings provided by LinkedIn help me to have complete control over my information on LinkedIn
- (3) I feel in control of who can see my information on LinkedIn

Self-disclosure (adapted from Krasnova and Veltri [36])

- (1) I have a comprehensive profile on LinkedIn
- (2) Professional and personal information about me found on LinkedIn would make it easier for others to understand me
- (3) I find time to keep my professional information on LinkedIn up-to-date

# **Data Availability**

Data is available on request from the authors.

## **Conflicts of Interest**

The authors declare that they have no conflicts of interest.

## References

- [1] AccessScience Editors, "The impact of social media," in *AccessScience*, McGraw Hill, 2016.
- [2] P. Li, H. Cho, and Z. H. Goh, "Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus," *Telematics and Informatics*, vol. 41, pp. 114–125, 2019.
- [3] J. Al-Menayes, "Dimensions of social media addiction among university students in Kuwait," *Psychology and Behavioral Sciences*, vol. 4, no. 1, pp. 23–28, 2015.
- [4] NapoleonCat, "LinkedIn users in Indonesia," 2019, https://napoleoncat.com/stats/linkedin-users-in-indonesia/2019/08.
- [5] Linkedin, "Perjanjian Pengguna," 2020, https://www.linkedin.com/legal/user-agreement?\_l=in\_ID.
- [6] M. C. Mendez and N. Lloret-Romero, Digital tools for academic branding and self-promotion, IGI Global, 2016.
- [7] S. Sameen and S. Cornelius, "Social networking sites and hiring: how social media profiles influence hiring decisions," *Journal of Business Studies Quarterly*, vol. 7, no. 1, pp. 27–35, 2013.
- [8] B. Shepherd, "Social recruiting: referrals," Workforce Management, vol. 92, no. 5, p. 18, 2013.
- [9] B. A. Brooks, "LinkedIn and your professional identity," *Nurse Leader*, vol. 17, no. 3, pp. 173–175, 2019.
- [10] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006.
- [11] L. N. Zlatolas, T. Welzer, M. Heričko, and M. Hölbl, "Privacy antecedents for SNS self-disclosure: the case of Facebook," *Computers in Human Behavior*, vol. 45, pp. 158–167, 2015.
- [12] J. Omarzu, "A disclosure decision model: determining how and when individuals will self-disclose," *Personality and Social Psychology Review*, vol. 4, no. 2, pp. 174–185, 2000.

- [13] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: why we disclose," *Journal of Information Technology*, vol. 25, no. 2, pp. 109–125, 2010.
- [14] L. Zhao, Y. Lu, and S. Gupta, "Disclosure intention of locationrelated information in location-based social network services," *International Journal of Electronic Commerce*, vol. 16, no. 4, pp. 53–90, 2012.
- [15] Z. Liu, Q. Min, Q. Zhai, and R. Smyth, "Self-disclosure in Chinese micro-blogging: a social exchange theory perspective," *Information and Management*, vol. 53, no. 1, pp. 53–63, 2016.
- [16] B. E. ALQadheeb and O. I. Alsalloum, "Self-disclosure in social networking sites in Saudi Arabia," *Journal of Business and Management*, vol. 13, no. 10, p. 96, 2018.
- [17] D. Clark, "How to brand yourself in Asia," 2015, Accessed on: 15 March 2023, https://www.linkedin.com/pulse/how-brand-yourself-asia-dorie-clark/.
- [18] V. Paramarta, M. Jihad, A. Dharma, I. C. Hapsari, P. I. Sandyaduhita, and A. N. Hidayanto, "Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: facebook, twitter, and instagram," in 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 271–276, Yogyakarta, Indonesia, 2018.
- [19] D. M. Boyd and N. B. Ellison, "Social network sites: definition, history, and scholarship," *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 210–230, 2007.
- [20] S. M. Jourard and P. Lasakow, "Some factors in self-disclosure," *Journal of Abnormal and Social Psychology*, vol. 56, no. 1, pp. 91–98, 1958.
- [21] H. Y. Huang, "Examining the beneficial effects of individual's self-disclosure on the social network site," *Computers in Human Behavior*, vol. 57, pp. 122–132, 2016.
- [22] J. J. Cameron, J. G. Holmes, and J. D. Vorauer, "When self-disclosure goes awry: negative consequences of revealing personal failures for lower self-esteem individuals," *Journal of Experimental Social Psychology*, vol. 45, no. 1, pp. 217–222, 2009.
- [23] N. C. Krämer and S. Winter, "Impression management 2.0," *Journal of Media Psychology*, vol. 20, no. 3, pp. 106–116, 2008.
- [24] N. Ellison, R. Heino, and J. Gibbs, "Managing impressions online: self-presentation processes in the online dating environment," *Journal of Computer-Mediated Communication*, vol. 11, no. 2, pp. 415–441, 2006.
- [25] S. E. Chang, A. Y. Liu, and W. C. Shen, "User trust in social networking services: a comparison of Facebook and LinkedIn," *Computers in Human Behavior*, vol. 69, pp. 207–217, 2017.
- [26] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Communications Surveys & Tutorials*, vol. 3, no. 4, pp. 2–16, 2000.
- [27] T. Mini, Privacy Calculus, School of Business, Economics and Information Systems, University of Passau, Passau, Germany, 2017.
- [28] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: a multidimensional developmental theory," *Journal of Social Issues*, vol. 33, no. 3, pp. 22–42, 1977.
- [29] B. R. Schlenker and S. A. Wowra, "Carryover effects of feeling socially transparent or impenetrable on strategic self-presentation," *Journal of Personality and Social Psychology*, vol. 85, no. 5, pp. 871–880, 2003.
- [30] K. Grissa, "What "uses and gratifications" theory can tell us about using professional networking sites (E.G. LinkedIn,

- Viadeo, Xing, SkilledAfricans, Plaxo...)," in *Digital Economy. Emerging Technologies and Business Innovation. ICDEc 2017*, pp. 15–28, Springer, 2017.
- [31] B. Florenthal, "Applying uses and gratifications theory to students' LinkedIn usage," *Young Consumers*, vol. 16, no. 1, pp. 17–35, 2015.
- [32] B. L. Berkelaar and P. M. Buzzanell, "Online employment screening and digital career capital," *Management Communication Quarterly*, vol. 29, no. 1, pp. 84–113, 2015.
- [33] I. Altman and D. A. Taylor, Social Penetration: The Development of Interpersonal Relationships, Holt, Rinehart & Winston, New York, NY, USA, 1973.
- [34] H. Krasnova, E. Kolesnikova, and O. Guenther, ""It won't happen to me!": self-disclosure in online social networks," in *AMCIS 2009 Proceedings*, pp. 1–10, Atlanta, GA, USA, 2009.
- [35] T. Wang, T. D. Duong, and C. C. Chen, "Intention to disclose personal information via mobile applications: a privacy calculus perspective," *International Journal of Information Management*, vol. 36, no. 4, pp. 531–542, 2016.
- [36] H. Krasnova and N. F. Veltri, "privacy calculus on social networking sites: explorative evidence from Germany and USA," in 2010 43rd Hawaii International Conference on System Sciences, pp. 1–10, Honolulu, HI, USA, 2010.
- [37] N. Bol, T. Dienlin, S. Kruikemeier et al., "Understanding the effects of personalization as a privacy calculus: analyzing selfdisclosure across health, news, and commerce contexts," *Journal of Computer-Mediated Communication*, vol. 23, no. 6, pp. 370–388, 2018.
- [38] M. El Ouirdi, J. Segers, A. El Ouirdi, and I. Pais, "Predictors of job seekers' self-disclosure on social media," *Computers in Human Behavior*, vol. 53, pp. 1–12, 2015.
- [39] X. Zhao, N. Salehi, S. Naranjit, S. Alwaalan, S. Voida, and D. Cosley, "The many faces of facebook: experiencing social media as performance, exhibition, and personal archive," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1–10, Paris, France, 2013.
- [40] Z. Jiang, C. S. Heng, and B. C. F. Choi, "Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions," *Information Systems Research*, vol. 24, no. 3, pp. 579–595, 2013.
- [41] S. Trepte, M. Scharkow, and T. Dienlin, "The privacy calculus contextualized: the influence of affordances," *Computers in Human Behavior*, vol. 104, p. 106115, 2020.
- [42] R. Chen and S. K. Sharma, "Self-disclosure at social networking sites: an exploration through relational capitals," *Information Systems Frontiers*, vol. 15, no. 2, pp. 269–278, 2013.
- [43] W. Y. Lin, X. Zhang, H. Song, and K. Omori, "Health information seeking in the web 2.0 age: trust in social media, uncertainty reduction, and self-disclosure," *Computers in Human Behavior*, vol. 56, pp. 289–294, 2016.
- [44] A. Joinson and C. B. Paine, "Self-disclosure, privacy and the Internet," in Oxford Handbook of Internet Psychology, pp. 237– 252, OUP, Oxford, UK, 2007.
- [45] C. Mutimukwe, E. Kolkowska, and Å. Grönlund, "Information privacy in e-service: effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior," *Government Information Quarterly*, vol. 37, no. 1, p. 101413, 2020.

- [46] P. A. Pavlou, "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101–134, 2003.
- [47] C. Dwyer, S. Hiltz, and K. Passerini, Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpaceAMCIS 2007 Proceedings, p. 339, Keystone, Colorado, USA, 2007.
- [48] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.
- [49] M. Jozani, E. Ayaburi, M. Ko, and K. K. R. Choo, "Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective," *Computers in Human Behavior*, vol. 107, p. 106260, 2020.
- [50] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia," *Computers in Human Behavior*, vol. 28, no. 6, pp. 2366–2375, 2012.
- [51] R. V. Labaree, Quantitative Methods Organizing Your Social Sciences Research Paper, University of Southern California, 2020.
- [52] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2–24, 2019.
- [53] J. F. Hair Jr., W. C. Black, B. J. Babin, and R. E. Anderson, "Multivariate data analysis," *Journal of the Royal Statistical Society. Series A (General) 7th ed*, vol. 136, no. 1, 2014.
- [54] S. Santoso, Konsep Dasar dan Aplikasi SEM dengan Amos 24, Elex Media Komputindo, Jakarta, Indonesia, 2018.
- [55] P. W. Handayani, Konsep CB-SEM dan SEM-PLS: disertai dengan contoh kasus, Rajawali Pers, Jakarta, Indonesia, 2019.
- [56] J. Davis, H. G. Wolff, M. L. Forret, and S. E. Sullivan, "Net-working via LinkedIn: an examination of usage and career benefits," *Journal of Vocational Behavior*, vol. 118, p. 103396, 2020.
- [57] G. O. A. Ampong, A. Mensah, A. S. Y. Adu, J. A. Addae, O. K. Omoregie, and K. S. Ofori, "Examining self-disclosure on social networking sites: a flow theory and privacy perspective," *Behavioral Sciences*, vol. 8, no. 6, p. 58, 2018.
- [58] S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press, 2002.
- [59] K. Mukaromah, A. Kusyanti, and A. R. Perdanakusuma, Analisis Faktor-Faktor Yang Memengaruhi Pengguna Snapchat Membagikan Video Dengan Menggunakan Structural Equation Modeling, Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2017.
- [60] A. Ningroem, A. Kusyanti, and R. Rokhmawati, "Analisis Faktor-Faktor Yang Mempengaruhi Self Disclosure Oleh Pengguna Facebook Dengan Menggunakan Structural Equation Modeling (SEM)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 2, no. 5, pp. 1970–1979, 2017.