Proceeding
Jogjakarta Communication Conference
Volume 1, No 1, pp. 114-125
ISSN 2988-5523

Understanding the Impact of Privacy Calculus on Social Media Self-disclosure: A Conceptual Framework and Research Proposition

Zhu Luhui*, Bahiyah Omar

School of communication, Universiti Sains Malaysia, Penang, Malaysia

*Corresponding author's email: zhuluhui@student.usm.my

ABSTRACT

Keywords

Privacy Calculus
Self-Disclosure
Social Media

Most social media platforms are encouraging users to disclose as much as possible due to self-disclosure on social media being the key value to the success of these platforms. Yet, when privacy breaches grow more and more frequent, individuals tend to do privacy calculations before self-disclosure. There are many factors that impact user self-disclosure behavior. On the basis of the privacy calculus theory, we developed a conceptual model to investigate the impact of perceived benefits and perceived risks on social media self-disclosure and proposed related research propositions, with the aim of revealing the impact mechanism of privacy calculus on social media self-disclosure and examining the effects of trust in platform, information sensitivity, privacy settings, and government regulation on user privacy calculus. Theoretically, the contribution of this study is the development of a privacy calculus model that reveals the user's privacy decision-making process. In terms of practical significance, this study may assist social media providers in better understanding users' privacy choices, decreasing privacy concerns, and enhancing user self-disclosure.

1. Introduction

With the rise of the internet and the maturity of communication technology, disclosing information on social media has become one of the most popular online activities in the current digital era (Apuke & Omar, 2021; Whiting & Williams, 2013). According to a statistic from Kemp (2023), as of January 2023, 4.76 billion people are actively adopting social media tools daily, accounting for 59.4% of the world's total population. Another research predicts that digital life will continue in the post-Covid-19 era, and people will rely more on online tools like social media (Anderson et al., 2021). Activities on social media reveal user interests, views, and intentions and leave a lot of user data behind (Krasnova et al., 2010; Parker & Flowerday, 2021). Meanwhile, data and information are essential to the social media business model (Lee et al., 2022; Naous et al., 2019). By utilizing social media research tools such as opinion mining, sentiment analysis, and social networking, social media operators can continue to get enormous amounts of user data with their knowledge and consent and offer online personalization services to improve the level of users' satisfaction (Chen, 2018; Gandomi & Haider, 2015).

The fast-growing usage of social media for disclosing information brings benefits to service providers as well as users (Abu-Shanab & Khasawneh, 2013). Yet, privacy invasion also comes along with this. In the current study, privacy invasion implies that social media users have been exposed to search and seizure, creation of databases consisting of personal information, and secondary usage of that information by a third party (Mekovec, 2010). Of all the privacy invasion cases, social media was declared the platform with the most privacy leakages. According to a survey of 1,000 United States

citizens (Proton, 2022), social media platforms have the highest percentage (42.12%) of people affected by privacy breaches, followed by gaming (25%) and tech-based websites (20.55%).

Such high levels of users data breaches on social media platforms have caused corresponding increased concerns about privacy and information security, encouraging researchers and practitioners to continuously study how to maintain an optimal balance between encouraging users' self-disclosure on social media on the most enormous scale and reducing concerns of privacy invasion to the utmost extent(Ma et al., 2021).

2. Problem Statement

Since social media service providers need to sustain their platform development and business growth, it is essential to understand the factors that are driving users' self-disclosure behaviors toward social media platforms (Cheung et al., 2014). Even though a growing amount of research has been conducted, the influencing factors on users' self-disclosure behavior remain poorly understood (Abramova et al., 2017).

Although previous studies on social media privacy concerns and self-disclosure behaviors have been abundant, there still exists a controversy (Cain & Imre, 2021). One line believes that there is little to no relationship between online privacy concerns and self-disclosure in social media settings. Hughes-Roberts (2013), based on a questionnaire survey and an examination of participants' Facebook profiles, concluded that a general statement of user privacy concern is not a valid indicator of disclosing behavior. Another line of research concluded that privacy concerns do matter in users' sharing behavior. Lutz et al. (2018) examined the disclosing–privacy relationship by exploring the privacy threats associated with internet-mediated self-disclosure and indicated that privacy concerns have an effect on disclosing intensity. The current study will continue to investigate the relationship between privacy concerns and self-disclosure based on privacy calculus theory to contribute to solving this academic controversy.

Researchers proposed that people always conduct a privacy calculus in their minds to make privacy decisions, in which process their behavior is determined by the result of the privacy trade-off (Chen, 2018; Jozani et al., 2020; Wang et al., 2020). Privacy calculus is a rigorous model to study privacy-related information disclosure behavior in the context of social media (Hassandoust et al., 2020). However, with regard to antecedents of privacy calculus, most studies were mainly performedfrom a sole aspect such as user factor, information factor, platform factor, or context factor, and few attempts have been made to develop a comprehensive study model for horizontally comparing the effect of these factors. Thus, it is necessary to further study the different influences of these factors on the choice of privacy calculus to better understand its mechanism of impacting social media self-disclosure.

3. Research Questions and Proposes

The main research objective of this conceptual paper is to investigate the antecedents of privacy calculus, namely the user factor, information factor, platform factor, and context factor, and their impact on social media self-disclosure. The specific research objectives are as follows.

1. To what extent do the user, information, platform, and context factors affect privacy calculus?
2. To what extent do the user, information, platform, and context factors affect users' self-disclosure on social media?
3. How does privacy calculus influence users' self-disclosure on social media?

This study is to develop a conceptual framework by proposing the relationship between these four factors (user, information, platform, context), privacy calculus, and social media self-disclosure, and horizontally compare the effect of these factors.

4. Literature Review and Propositions Development

In past research, self-disclosure refers to individuals tend to disclose all sorts of information, including descriptive, evaluative, and affective information, about the self, opinions, or attitudes that they may communicate to another person (Kreiner & Levi-Belz, 2019). The topic of self-disclosure has been researched from a variety of disciplinary perspectives for decades. From the social science disciplines, researchers consider self-disclosure as a social exchange process in which individuals evaluate cost and benefit before they communicate with others (Worthy et al., 1969).

4.1 Privacy Calculus Theory

In 1999, Culnan and Armstrong (1999) first came up with the "privacy calculus," which argued that, in the context of purchasing products and services, people always conduct a calculus between perceived benefits and the potential costs in their mind to make a privacy decision before they disclose the personal information which is necessary to complete a transaction. Privacy calculus theory provides an explanation that personal information can be regarded as the economic value of the transaction(Beldad et al., 2011; Murphy, 2017); The main philosophy of privacy calculus theory is that the user's tradeoff between perceived benefits and perceived risks(Dinev et al., 2006; Dinev & Hart, 2006; Li et al., 2010; Liu et al., 2014). Li and Wu (2022) suggested the following formula for privacy calculus theory: U(X)=Benefits-Cost, which describes the decision-making process of personal information disclosing behavior as a "benefit"-"risk" calculation.

This theory was initially applied to commercial environments to explore the intention of individuals to disclose information for targeted advertising (Culnan & Armstrong, 1999) and later for e-commercial transactions (Dinev & Hart, 2006). Krasnova et al. (2010) were the first to analyze the privacy calculus in the context of online social media platforms; they found that users who reported having higher perceived privacy risks had a less comprehensive Facebook profile and users who reported getting more benefits had a more comprehensive profile. Subsequently, many researchers have applied this perspective to explain the individual's decision as the result of weighing the costs and benefits of information disclosure in various online contexts.

4.2 The Impact of Privacy Calculus on Social Media Self-disclosure

The privacy calculus model has provided a sound framework to analyze information disclosure behavior. As mentioned above, the main principle of privacy calculus theory is that the user's tradeoff between perceived benefits and perceived risks(Dinev et al., 2006; Dinev & Hart, 2006; Li et al., 2010; Liu et al., 2014), these two constructs should respectively have positive and negative impacts on individuals' privacy choices and self-disclosing behavior(Sun et al., 2015).

Specifically, when users disclose their personal information with their friends on social media platforms, they may get some benefits such as feeling secure(Arpaci, 2020) due to trust in the platform, getting personalization services(Merten, 2021; Tucker, 2014), and earning social capital(Apuke & Omar, 2021; Ellison et al., 2011; Liu & Brown, 2014). These benefits will drive users to disclose their personal information to obtain these benefits. On the other hand, because privacy-related information is more sensitive than other types of information, users may be worried about their personal information being misused by others and do not want to share the information (Bol et al., 2018; Martin et al., 2017). Thus, we propose that:

H1. Perceived benefits are positively associated with users' social media self-disclosure behavior.

H2. Perceived risks are negatively associated with users' social media self-disclosure behavior.

4.3 The Influencing Factors of Privacy Calculus

Previous research has examined the influencing factors of privacy calculus and self-disclosure in many contexts, but most studies were mainly performed from a sole aspect (Li & Wu, 2022) or divided the influencing factors into endogenous and exogenous factors conflicting with each other (Kroll & Stieglitz, 2021). Since self-disclosure on social media involves personal information posted by individuals on social media platforms in a certain social context, this study considers the antecedent effects of user factor, platform factor, information factor, and context factor on privacy calculus, and

further studies the different influences of these factors on the choice of privacy calculus to better understand its mechanism of impacting social media self-disclosure.

4.3.1 Trust in Platform as a User Factor

Trust is usually adopted as a strong predictor of privacy behaviors (Dwyer et al., 2007; Widjaja et al., 2019; Wu et al., 2012), and it has been shown to be a way to decrease concern about the risks of privacy and encourage users to engage in social media (Metzger, 2004). In this study, trust refers to trusting beliefs (McKnight et al., 2002), and it is defined as a user's overall trust in social media service providers (Widjaja et al., 2019). The level of trust is uncertain so it might lead to different privacy choices (Martin, 2013). Prior studies have empirically shown that trust serves as a risk-reducing factor (Gefen et al., 2003; Kulkarni, 2022) and can help to improve users' satisfaction (Maqableh et al., 2021). In contrast, if users lose trust in social media platforms, their perceived privacy risk toward self-disclosure is likely to increase (Kroll & Stieglitz, 2021; Tsay-Vogel et al., 2018). Thus, we propose that:

H3a: Trust in Platform is positively associated with perceived benefits.

H3b. Trust in Platform is negatively associated with perceived risks.

4.3.2 Information Sensitivity as an information factor

Information sensitivity is defined as the level of privacy concerns that people perceive for a type of information in a certain context (Weible, 1993; Widjaja et al., 2019). It has been widely recognized that the type of information collected and used by social media affects the level of individuals' privacy concerns (Dinev et al., 2013; Li et al., 2016; Malhotra et al., 2004). More sensitive information will be perceived as riskier and more uncomfortable to disclose (Dinev et al., 2013; Li et al., 2011) since certain spheres of life are seen as more private than others. Considering the fact that users' privacy concerns vary dramatically by the degree of sensitivity of the information, this study proposes that:

H4a: Information sensitivity is negatively associated with perceived benefits.

H4b. Information sensitivity is positively associated with perceived risks.

4.3.3 Privacy Setting as a platform factor

In the social media context, perceived affordance has become the major factor driving perceived benefits and disclosure intentions. Such affordance enables social media users to cope with complex privacy and security issues through privacy settings (Santos & Faure, 2018). For instance, Shane-Simpson et al. (2018) demonstrated that user-adjustable privacy settings could promote the social capital of users and increase, rather than decrease, the information they disclose. Moreover, providing users with alternative information disclosure options will enhance users' perceived fairness and security of the program setting and increase their perceived controllability over personal privacy information (Ma et al., 2021; Wang & Wu, 2014). Ma et al. (2021) further indicated that the privacy settings of "Last Three Days/One Month/Six Months Visibility" on WeChat Moment significantly impacted users' self-disclosure intentions by counteracting perceived privacy risks and positively affected the perceived benefits. Hence, this study proposes that:

H5a: Privacy setting is positively associated with perceived benefits.

H5b. Privacy setting is negatively associated with perceived risks.

4.3.4 Government regulation as a context factor

Government regulation in the current study refers to the government regulating online platforms to protect users' personal information from data breaches and misuse (Dinev et al., 2008). Previous privacy-related studies indicated that legislation is one of the significant and most commonly used approaches to protecting information privacy from the perspective of the government (Xu et al., 2009; Xu et al., 2014). Government regulation assuages users' perceived privacy risks by ensuring that their personal information is treated in a respectful and fair manner (Lasprogata & King, 2004; Sarathy & Robertson, 2003). Recognizing the deterrent value of a legal system, users tend to believe that social

media service providers would conform to government regulation, and would therefore collect and use personal information appropriately (Xu et al., 2014). In addition, privacy protection standards set by the government allow users to believe that service providers will protect their disclosed information post-contractually, thereby increasing their sense of security over personal information (Tang et al., 2008). Hence, this study hypothesizes that：

H6a: Government regulation is positively associated with perceived benefits.

H6b. Government regulation is negatively associated with perceived risks.

5. Conceptual Framework

This conceptual paper posits the mechanism through which the privacy calculus influences users' self-disclosure behavior in social media, based on the preceding discussions. The process of privacy calculus is influenced by a number of factors (Jozani et al., 2020; Kang & Namkung, 2019), and this conceptual paper provides propositions regarding this subject from four aspects, forming the following conceptual framework.

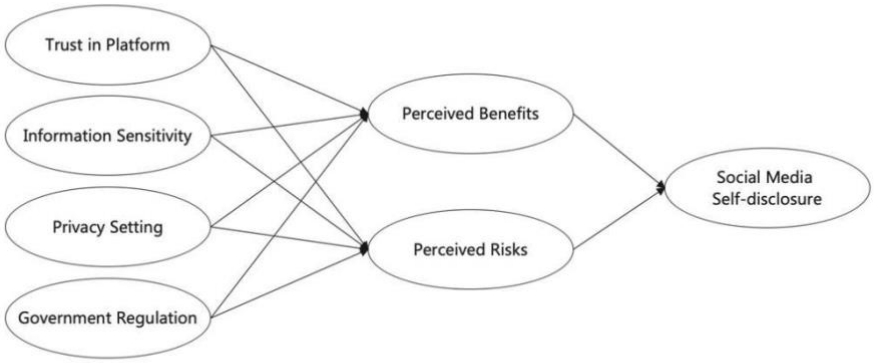

Figure 1. Conceptual Framework

6. Research Methodology

This conceptual framework involves predicting relationships and building connecting relationships between many independent variables. To statistically validate this conceptual model, it should be tested empirically. According to Babbie (2020), quantitative methodology assists in unbiased and deductive reasoning of postulation and offers a generalization of the research outcome. The survey method is considered the best way for this research due to the large population making it difficult to have direct observations of the subjects under examination (Nardi, 2018). The data obtained from the survey enabled this study to have statistical reports that were used to project the outcomes of the disclosing behaviors of the people. Therefore, a survey method for the collection of data from the respondents is needed.

Sampling is the process of selecting a sample from the population (Kumar & Semetko, 2018). Etikan et al. (2016) suggested that when the population of interest is difficult to reach and compiling the list of the population seems problematic, non-probability sampling should be utilized. Since the overall population size exceeds 100,000 (Hair et al., 2019), this study will adopt the nonprobability sampling and virtual snowball sampling approach to obtain a more representative sample of the population to generate the result that will reflect the true features of the population.

This study will make use of a self-administered online survey questionnaire as its instrument. All the questions can be adapted from validated variables found in prior studies, and re-reworded to suit the context of this current investigation. Measurement for perceived benefits and perceived risks can be drawn from (Wang et al., 2020) and (Kim et al., 2019). Items of trust in platform, information sensitivity, privacy setting, and government regulation can be adopted from (Naous et al., 2019), (Jozani et al., 2020), (Cheung et al., 2014), and (Xu et al., 2011), respectively. Similarly, measures of

social media self-disclosure stem from (Sharif et al., 2021). All the items are listed in the following table 1.

Table 1. Measurement Items and Sources of Constructs

Construct	Measurement Items	Source
Perceived Benefits	1: Self-disclosure on social media may help to establish relationship with my friends.	(Wang et al., 2020)
	2: Self-disclosure on social media may help to gain emotional support from others.	
	3: Self-disclosure on social media may help me joining in some social groups.	
	4: Self-disclosure on social media may receive coupons, discounts and cash rewards.	
Perceived Risks	1: The information I disclosed on social media could be sold to third parties.	(Kim et al., 2019)
	2: The information I disclosed on social media could be misused.	
	3: The information I disclosed on social media could be made available to unknown individuals or companies without my knowledge.	
	4:The information I disclosed on social media could be made available to governmental agencies.	
	5: The information I disclosed on social media could be jeopardized by hacking activities.	
Trust in Platform	1: I believe that the social media platform would act in my best interest when dealing with my personal information.	(Lo & Riemenschneider, 2010)
	2: The social media platform is interested in protecting my personal information according to the preferences I specify.	
	3: The social media platform would fulfill its promises related to the personal information provided by me.	
	4: The social media platform is sincere and genuine in managing my personal information.	
	5: The social media platform handles personal information submitted by users in a competent fashion.	
	6: The social media platform performs its role of managing my personal information according to my privacy settings very well.	
Information Sensitivity	1: I do not feel comfortable with the type of information social media platforms request from me.	(Jozani et al., 2020)
	2: I feel that social media platforms gather highly personal information about me.	
	3: The information I provide to social media platforms is very sensitive to me.	
Privacy Setting	1: I feel in control over the information I disclose on social media via privacy settings.	(Cheung et al., 2014; Krasnova et al., 2010)
	2: Privacy settings allow me to have full control over the information I disclosed on social media.	

	3: I feel in control over who can view my information on social media via privacy settings.	
Government Regulation	1. I believe that the government should protect me from the misuse of my personal data by social media platforms.	(Gong et al., 2019)
	2. I believe that the government should govern and interpret the practice of how social media platforms collect, use, and protect my private information.	
	3. I believe that the government should be able to address the violation of the information I disclosed to social media platforms.	
Social Media Self-disclosure	1: I share my personal information (such as real name, current town, education, employment, and so on) on my social media.	(Sharif et al., 2021)
	2: I have my contact information (such as email, cell phone number, address, and so on) on my social media.	
	3: I share my personal pictures on my social media.	
	4: I share my personal videos on my social media.	
	5: I share my ideas, opinions, and recommendations through my social media.	

With regard to data analysis, two statistical methods can be used in this study. One of them is the Statistical Package for the Social Sciences (SPSS), which can be utilized for data imputation, screening, and a descriptive analysis of the respondent's demographic characteristics. Another is PLS-SEM, which is suitable for the identification of complex critical structural models, so Smart PLS 4 can be used to test the measurement model and the structural model.

7. Conclusion

This paper has successfully developed a theoretical framework that is helpful for future research in privacy calculus and self-disclosure. Theoretically, this conceptual paper proposes a conceptual framework to explain the decision-making process related to privacy issues on social media based on the privacy calculus theory. Besides, this study has provided a new insight view on privacy calculus studies by adopting user, information, platform, and context factors as antecedents. Practically, understanding these factors and their impact may promote the self-disclosure behavior of users, which will help social media operators provide users with satisfactory services while better protecting their privacy.

Even though the framework is established, there is still a need for more efforts in the future. Firstly, the survey mentioned above needs to be conducted to get data for users, because the conceptual framework and propositions must be tested to identify them. Secondly, privacy calculus is a complex process and can be impacted by user factors, information factors, platform factors, and context factors, this study only adopts one construct of each factor, and more factors need to be further investigated in this area.

8. References

Abramova, O., Wagner, A., Krasnova, H., & Buxmann, P. (2017). Understanding self-disclosure on social networking sites-a literature review.

Abu-Shanab, E., & Khasawneh, R. T. (2013). E-Government and Social Media Sites- The Role and Impact. *World Journal of Computer Application and Technology 1*(1), 10-17. https://doi.org/10.13189/wjcat.2013.010103

Anderson, J., Rainie, L., & Vogels, E. A. (2021). *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges*

https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

Apuke, O. D., & Omar, B. (2021). What drives news sharing behaviour among social media users? A relational communication model from the social capital perspective. *International Sociology, 36*(3), 339-361. https://doi.org/10.1177/0268580920961323

Arpaci, I. (2020). What drives students' online self-disclosure behaviour on social media? A hybrid SEM and artificial intelligence approach. *Int. J. Mob. Commun.*, *18*(2), 229-241.

Babbie, E. R. (2020). *The practice of social research*. Cengage learning.

Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, *27*(6), 2233-2242.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . . De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370-388.

Cain, J. A., & Imre, I. (2021). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, *0*(0). https://doi.org/https://doi.org/10.1177/14614448211000327

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American behavioral scientist*, *62*(10), 1392-1412.

Cheung, C., Lee, Z. W., & Chan, T. K. (2014). Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. *Internet Research*.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy online* (pp. 19-32). Springer.

Etikan, I., Alkassim, R., & Abubakar, S. (2016). Comparision of snowball sampling and sequential sampling technique. *Biometrics and Biostatistics International Journal*, *3*(1), 55.

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137-144.

Gefen, D., Rao, V. S., & Tractinsky, N. (2003). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. HICSS,

Gong, X., Zhang, K. Z., Chen, C., Cheung, C. M., & Lee, M. K. (2019). What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity. *Information Technology & People*.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European business review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2020). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463-471. https://doi.org/10.1093/jamia/ocaa240

Hughes-Roberts, T. (2013, 8-14 Sept. 2013). Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour? 2013 International Conference on Social Computing,

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, 106260. https://doi.org/https://doi.org/10.1016/j.chb.2020.106260

Kang, J.-W., & Namkung, Y. (2019). The role of personalization on continuance intention in food service mobile apps: A privacy calculus perspective. *International Journal of Contemporary Hospitality Management*.

Kemp, S. (2023). *DIGITAL 2023: GLOBAL OVERVIEW REPORT* https://datareportal.com/reports/digital-2023-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=China&utm_content=Global_Overview_Link

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281. https://doi.org/https://doi.org/10.1016/j.chb.2018.11.022

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109-125.

Kreiner, H., & Levi-Belz, Y. (2019). Self-disclosure here and now: combining retrospective perceived assessment with dynamic behavioral measures. *Frontiers in psychology*, *10*, 558.

Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: improving decisions about self-disclosure in social networks. *Behaviour & Information Technology*, *40*(1), 1-19. https://doi.org/10.1080/0144929X.2019.1584644

Kulkarni, S. (2022). Regulation of reviews and product ratings: A tool for consumer trust? *Regulation*, *20*(1), 199-198.

Kumar, A., & Semetko, H. A. (2018). Peace communication in cross-border media flows. *Journal of Communication*, *68*(3), 612-635.

Lasprogata, G., & King, N. J. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev.*, 4.

Lee, C. B., Io, H. N., & Tang, H. (2022). Sentiments and perceptions after a privacy breach incident. *Cogent Business & Management*, *9*(1), 2050018. https://doi.org/10.1080/23311975.2022.2050018

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62-71.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics*, *88*, 8-17.

Li, J., & Wu, J. (2022). Study on the Influence Mechanism of the Third-Person Effect(TPE) on Privacy Protection Behavior: Findings from PLS and fsQCA [第三人效应对个体隐私保护行为的影响机制研究——来自 PLS 与 fsQCA 的研究发现]. *Information Research*, *294*(4). https://doi.org/10.3969/j.issn.1005-8095.2022.04.004

Liu, D., & Brown, B. B. (2014). Self-disclosure on social networking sites, positive feedback, and social capital among Chinese college students. *Computers in Human Behavior*, *38*, 213-219. https://doi.org/https://doi.org/10.1016/j.chb.2014.06.003

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014, 6-9 Jan. 2014). Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications. 2014 47th Hawaii International Conference on System Sciences,

Lo, J., & Riemenschneider, C. (2010). An examination of privacy concerns and trust entities in determining willingness to disclose personal information on a social networking site.

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society*, *21*(10), 1472-1492. https://doi.org/10.1080/1369118X.2017.1339726

Ma, X., Qin, Y., Chen, Z., & Cho, H. (2021). Perceived ephemerality, privacy calculus, and the privacy settings of an ephemeral social media site. *Computers in Human Behavior*, *124*. https://doi.org/10.1016/j.chb.2021.106928

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Maqableh, M., Hmoud, H. Y., Jaradat, M., & Masa'deh, R. (2021). Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction. *Heliyon*, *7*(9), e07899. https://doi.org/10.1016/j.heliyon.2021.e07899

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of marketing*, *81*(1), 36-58.

Martin, K. E. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*, *18*(12-2).

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

Mekovec, R. (2010). Online privacy: overview and preliminary research. *Journal of information and organizational sciences*, *34*(2), 195-209.

Merten, L. (2021). Block, hide or follow—personal news curation practices on social media. *Digital Journalism*, *9*(8), 1018-1039.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), JCMC942.

Murphy, R. S. (2017). Property rights in personal information: An economic defense of privacy. In *Privacy* (pp. 43-79). Routledge.

Naous, D., Kulkarni, V., Legner, C., & Garbinato, B. (2019). Information Disclosure in Location-based Services: An Extended Privacy Calculus Model. ICIS,

Nardi, P. M. (2018). *Doing Survey Research: A Guide to Quantitative Methods (4th ed.)*. Routledge. https://doi.org/https://doi.org/10.4324/9781315172231

Parker, H. J., & Flowerday, S. (2021). Understanding the disclosure of personal data online. *Information & Computer Security*, *29*(3), 413-434. https://doi.org/10.1108/ICS-10-2020-0168

Proton. (2022). *US data protection: Online habits and data breaches* https://protonvpn.com/blog/us-data-protection-habits/

Santos, M., & Faure, A. (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption. *Social Media+ Society*, *4*(3), 2056305118795876.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*(2), 111-126.

Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior*, *86*, 276-288. https://doi.org/https://doi.org/10.1016/j.chb.2018.04.041

Sharif, A., Soroya, S. H., Ahmad, S., & Mahmood, K. (2021). Antecedents of self-disclosure on social networking sites (snss): A study of facebook users. *Sustainability*, *13*(3), 1220.

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278-292. https://doi.org/https://doi.org/10.1016/j.chb.2015.06.006

Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, *24*(4), 153-173.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141-161. https://doi.org/10.1177/1461444816660731

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of marketing research*, *51*(5), 546-562.

Wang, L., Hu, H.-H., Yan, J., & Mei, M. Q. (2020). Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, *33*(2), 353-380. https://doi.org/10.1108/JEIM-05-2019-0121

Wang, S.-C., & Wu, J.-H. (2014). Proactive privacy practices in transition: Toward ubiquitous services. *Information & Management*, *51*(1), 93-103. https://doi.org/https://doi.org/10.1016/j.im.2013.09.005

Weible, R. J. (1993). *Privacy and data: An empirical study of the influence of types of data and situational context upon privacy perceptions*. Mississippi State University.

Whiting, A., & Williams, D. (2013). Why people use social media: a uses and gratifications approach. *Qualitative Market Research: An International Journal*, *16*(4), 362-369. https://doi.org/10.1108/QMR-06-2013-0041

Widjaja, A. E., Chen, J. V., Sukoco, B. M., & Ha, Q.-A. (2019). Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. *Computers in Human Behavior*, *91*, 167-185.

Worthy, M., Gary, A. L., & Kahn, G. M. (1969). Self-disclosure as an exchange process. *Journal of personality and social psychology*, *13*(1), 59-63. https://doi.org/10.1037/h0027990

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889-897.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2009). Effectiveness of Privacy Assurance Approaches in Location-Based Services: A Study of India and the United States. 2009 Eighth International Conference on Mobile Business,

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2014). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, *26*(3), 135-174. https://doi.org/10.2753/mis0742-1222260305