User Behavior in Social Networks Toward Privacy and Trust: Literature Review

https://doi.org/10.3991/ijim.v16i01.27763

Razan Saleh Almogbel(✉), Ali Abddulaziz Alkhalifah
College of Computer, Qassim University, Buraydah, Saudi Arabia
411200003@qu.edu.sa

Abstract—Social networks (SNs) have become a significant part of daily life. It has become one of the most effective ways in which people communicate with each other. Huge amounts of data are generated and shared through SNs worldwide, where users share their personal and sensitive information. Therefore, disclosure of private information or identity and the loss of trust among users are among the most prominent and widespread privacy concerns. The main target of this study is to investigate the relationship between privacy, trust, and their effects on user behavior on the Social networks. It provides a detailed and overall overview of the concepts and methods related to protecting privacy and enhancing trust in Behavioral SNs users. In addition, it illustrates many of the key aspects of the research in the context of identity privacy and trust in users' behavior on SNs and shows the most important restrictions and gaps that have been found and guidance on future research directions.

Keywords—social networks (SNs), privacy, trust, user behavior

1 Introduction

SNs like Facebook, Twitter, and LinkedIn have grown in importance in our online life in recent years and continue to do so at an alarming rate. Moreover, based on [1], in 2020, the total number of users of various SNs worldwide has over 3.6 billion, which means the global use of social media rate raised at 49 percent, where Facebook is considered to become the most popular SN worldwide, it presently has a monthly active user base of almost 2.5 billion. Besides, the direction of making SNs allowed for multifunctional features like social learning, social health, social fitness, and social payment applications, has aggravated the users' privacy concerns.

SNs users communicate with each other and share private and personal details which others can misuse the sensitive information of users, giving rise to identity privacy concerns of individuals in SNs. This privacy concern placed users at potential risk, which led to loss of trust. Therefore, users need to be capable of preserving their privacy without leaving unwanted traces of their online activities. Identity privacy depends largely

on the intention of user to disclose personal and sensitive information and interact with other users and thus affect trust.

Usually, present-day methods to defining identity focus on defining it at one of three separate "levels": individual, relational, or collective [2], where individual identity refers to personal identity, which is characterized as forms of self-definition, such as goals, values, and beliefs, at the level of the person [3]. Relational identity indicates the characters of an individual, including identity contents, like parent, co-worker, spouse, customer, etc., with other individuals [3]. However, relational identity is often important to the concept and interpretation of these roles by the people who assume them [3]. Lastly, collective identity refers easily to "membership of any type of social group," such as race, nationality, gender, families, etc. It is likewise stressed that people can have material identities. People perceive and treat material objects as aspects of their identities, such as home, clothing, vehicles, and the contents of a bank account [3].

Moreover, trust is closely correlated to privacy, and trust may serve both as an antecedent and a consequence of privacy concerns, relying on the context in which it is used [4]. In several disciplines, trust has been studied. Each of these fields has identified and studied trust from many angles. each of these disciplines, and SNs might not be straight relevant to their definitions. So, according to [5,6] generally, trust is "a measure of confidence that an entity or entities will behave in an expected manner."

Figure 1 presented the growth of social networks in 2021 which leads to an increase in concerns about privacy and trust in social networks and thus leads to an increase in the volume of articles about privacy and also trust within social networks where describes the increasing academic interest in this field over recent years.

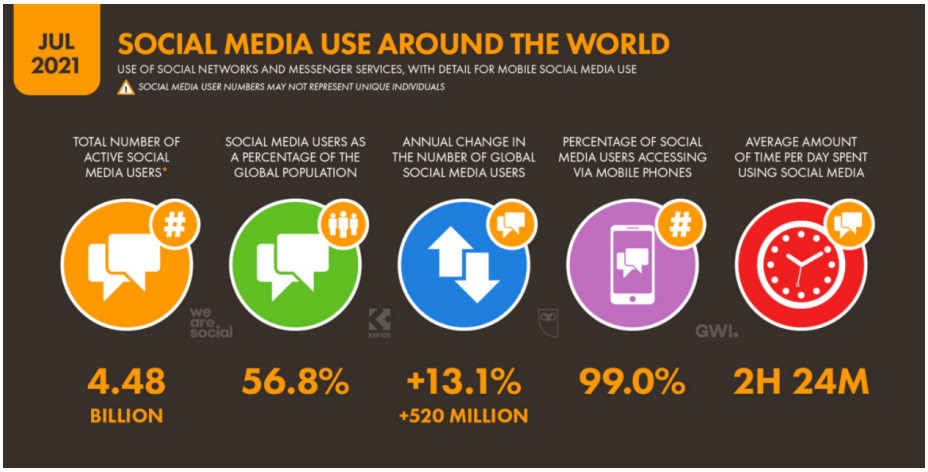

Fig. 1. The growth of social networks in 2021 [6]

And in this research paper will be determined what the existing methods and techniques used to protecting identity privacy and enhancing trust in behavioral SNs users are.

The rest of this paper is structured as follows. In section 2 shows the research methodology that will be followed. Section 3 analyzes a detailed literature review about the existing methods and techniques used to protect identity privacy and enhancing trust in behavioral SNs users. Discusses previous research papers, and the most important criticisms on them are highlighted in Section 4. Section 5 debates limitations and future research directions. Finally, concludes the paper.

2 Research methodology

In this paper, the method recommended by Moher et al. [7] and Kitchenham [8] will be followed. Based on their approach, three steps will be followed to systematically search for pertinent papers, which are: protocol development, research papers filtration by title, keywords, abstract, and data extracted from these selected papers.

2.1 Development of a protocol

A keyword search was used to find relevant publications in the literature. Several keyword searches were conducted, including Social Networks, Privacy, Trust, and User Behavior were searched through the Google Scholar and ScienceDirect databases. The papers published in English only were considered, and the research resulted in returning the most essential 13 articles that addressed about how to protect privacy and enhance trust in the behavior of users of SNs. This strategy that was followed in the research allowed access to noteworthy articles on this topic for a comprehensive review.

2.2 Research papers filtration by title, keywords, and abstract

All papers were analyzed and processed then revised based on their title, keywords, and abstracts to assure that they were valid and relevant where; the research offered a contribution to social networks about protecting privacy and building trust in users' behavior. The initial analysis yielded 63 articles generated 13 that were chosen as presenting robustly relevant for this study based on the inclusion criteria.

2.3 Extraction of data from the selected papers

For each research paper, the following information is extracted from the sources: date of publication, publication journal, author(s), and source(s) of the paper, as well as key findings and limitations. The data extracted from research papers includes the following: date of publication, publication journal name, key findings, and research limitations/gaps.

3 Related work

User privacy on social networking sites has recently received a lot of attention. This section will review the concepts and methods related to protecting identity privacy

and enhancing trust in users of behavioral SNs. Authors Wu et al. [9] mainly focused their study on the effect of the privacy policy content where they have seen how the content of privacy policies affects trust and privacy concerns, in addition to how trust and privacy concerns affect willingness to provide personal information online when cross-cultural factors are taken into account.

And centered on the Privacy–Trust–Behavioral Intention model, this study created a proposed model. The Privacy–Trust–Behavioral Intention model [10] is primarily focused on expectations in the United States. It explains the connection between Federal Trade Commission (FTC) dimensions, trust, and the intention to engage in online business activities. But this study expands the perception to other cultures, including Taiwan and Russia, to consider how the content of online privacy statements relates to customer trust and privacy concerns, along with how the respondents' various cultural contexts can moderate the findings. A total of 500 people took part in the survey, including 250 Russians and 250 Taiwanese. And this study tests seven research hypotheses.

Their study showed a link between the content of privacy policies and privacy concerns and trust, as well as a link between willingness to share personal data and privacy concerns and trust. There was also a major cross-cultural influence on the relationships between the privacy policies content and privacy concerns and trust. This study may need to investigate the effect of gender and age over privacy concerns and trust and the content of privacy policy. Besides can consider other factors that have a important effect on privacy and trust. Then, Taddei and Contena [11] contemplate examining the associations between privacy, trust, and control of explication for self-disclosure behaviors in online social networks.

Through the use of mediation and moderation techniques, the following three hypotheses are tested and found to be correct: (1) Perceived control directly impacts the perception of trust in SNs; the perception of trust in SNs influences the perception of privacy concerns, and this last variable has a mediation effect and is directly connected to the degree of online self-disclosure behavior; (2) Privacy concerns impact the degree of perceived control which, in turn, influences the perception of trust in SNs; and this final variable has a mediating effect and is strongly related to the degree of online self-disclosure activity. In addition, (3) privacy concerns offer a variable that can serve to mitigate the relationship between perceived control, general trust, and online self-disclosure activities that are associated with trust itself. After that, determine which of these three hypotheses is most likely to be able to explain the relationship between self-behaviors.

This study revealed the impact of the connection between privacy concerns and trust on online self-disclosure, as well as the lack of a direct impact of privacy concerns on disclosure itself. The definitions that they gave in this study for the studied variables are still under debate, where it was achieved in 2013.

Xu et al. [12] conducted a study in which they discovered the most important elements impacting users' self-disclosure of personal information. Through the use of privacy calculus, the perceived advantage was incorporated into the Theory of Planned Behavior. It was suggested explicitly for the context of social networking sites, with some modifications, that an integrated model be used.

They used the privacy calculus theory to determine when personal information should be disclosed since they were concerned about the privacy implications as well

as the alleged benefits. The Theory of Planned Behavior (TPB) model, on the other hand, is responsible for the development of the notions of behavior control, subjective norm, and components of the attitude. And based on these, they suggested hypotheses and gathered data using self-administered questionnaires.

Therefore, to the results, n the data analysis, it was discovered that perceived danger and information control both had a substantial impact on privacy concerns among participants. The items pertaining to information sensitivity, subjective norm, and privacy concern, on the other hand, did not pass the importance testing. However, it has the potential to uncover more elements that influence people's behavior choices. Furthermore, the sample used in this study was taken from a group of Chinese university students who participated in the study, so the findings may not be uniformly applicable.

Next came the authors Zlatolas et al. [13], who developed a model comprised a series of constructs: awareness of privacy, privacy control, privacy social norms, privacy policy, privacy concerns, self-disclosure, and privacy value to a better grasp of how privacy issues decide self-disclosure.

Awareness of privacy, privacy control, privacy social norms, privacy policy, privacy concerns, according to the model, all have a significant effect on the value of privacy, privacy concerns, and self-disclosure. Also, the model recommends that each of the four independent variables is related to the others. Furthermore, the model posits that the value of privacy and privacy concerns have a direct impact on the amount of information that people disclose on Facebook. And, on the basis of these constructs, they developed a set of hypotheses, which they tested using an online questionnaire that had 14 hypotheses in all.

The route analysis accepted 11 of the 14 hypotheses that were tested. According to the report, Facebook's self-disclosure is influenced by privacy social norms, privacy awareness, privacy policy, privacy concerns, and privacy values. The findings also revealed that the social norms of privacy, policies, and controls impact privacy value. While privacy concerns are influenced by privacy policy, privacy awareness, and privacy control. The findings cannot be applied to all Facebook users worldwide. And future research should look for and include potentially important constructs related to privacy and self-disclosure.

In another way, Malik et al. [14] the researchers investigated the effects of several factors of privacy connected with sharing the photo on Facebook, accordingly, the model is designed to demonstrate the relationship between trust and actual Facebook user action, as well as the relationship between privacy awareness, privacy worries, and privacy-seeking behavior. It studies how users' intentions to share images on Facebook are influenced by their trust and activity levels. And they made six hypotheses based on these constructs. Where collected the data using an online survey from Facebook users, then analyzed these data using partial least squares (PLS) path modeling.

In accordance with the findings, privacy awareness has the strongest link with trust of the three types of privacy-related behavior investigated. Another finding is that there is a high association between privacy awareness and actual Facebook usage. Furthermore, they demonstrate that, while privacy-seeking conduct has a significant positive association with Facebook activity, it has only a modest effect on trust in Facebook and other social media platforms. In contrast to their plans to participate in images, users' trust in and activity on Facebook were found to be strongly connected with their

intentions to participate in photos. The measuring model may also include constructs that address a user's privacy-related beliefs, expectations, and behaviors, as well as other constructs. And this study was limited to only one social networking, Facebook.

A study came as a comparison, and it compared between LinkedIn and Facebook with the purpose of learn more about the variables that impact users' trust in social networking services through Chang et al. [15].

They showed that both Facebook and LinkedIn trust approaches could be privacy concerns-based and possible risk, performance anticipation, and the user trust social influence and intention to continue using the service. There were several steps to this paper, including an expert questionnaire survey, the progression of the research model with nine hypotheses, questionnaire design, data collecting from respondents, and the analysis of the data collected. Along with the findings, perceived risk and privacy concerns had a greater influence on trust than effort expectancy and social influence. And users' trust in LinkedIn is influenced more by privacy concerns than users' trust in Facebook. However, Facebook's social influence on continuance intention is greater than LinkedIn's. However, this paper compares Facebook and LinkedIn, another type of social network with distinct user group characteristics.

In another way, Aghasian et al. [16] suggested a new way to improve privacy in friending, and they named the proposed: privacy-enhanced friending framework. This allows users to specify what they want to share with other people while minimizing the risk of being exploited. Therefore, the first step in this study to determine what kinds of data or attributes can generate privacy threats for users, they proposed a sensitivity calculation scheme. This is accomplished by assessing the risks to which users can be exposed, which is achieved by the Bernstein polynomial function proposed. Following this, a new model is then used to anonymize users participating in various social networks.

Appraisal reveals that, in addition to anonymization, calculating the sensitivity of information provides a more precise and accurate result for friending in a computationally active way. This study may need some contributions by conducting studies to examine the types of attacks that can be executed on anonymous data. Further research may examine how users perceive privacy, how they achieve privacy preferences on social networking websites, and how they make trade-offs between their privacy and their online presence in the future.

In the perspective of the Online Social Network, Heravi et al. [17] emphasized information privacy, which seeks to examine whether there is a distinction to be made between privacy behavior and privacy concern. And this study, therefore, regards privacy performance as both self-disclosure and the use of privacy-protective measures to obtain a deeper understanding of privacy behavior, it goes beyond simply using privacy settings and entails being cautious when joining groups, accepting requests from a friend, and becoming familiar with one's privacy settings

They have executed this research through two studies. The aim of study 1 was to explore the essential motives for the use of an online social network, where the main question was "What are the prominent motives for using an online social network?". And that in order of predominance, the motivations found were: 1-relationship maintenance, 2-relationship building, 3-entertainment, and 4-seeking for information. Relationship maintenance was the most widely identified motivation for using online

social networks. Alternatively, the aim of Study 2 was two-fold: first, examine whether the reasons for using online social networks affect information privacy concerns, and second, analyze whether data privacy concerns affect online social network privacy behavior.

Two variables were used to investigate privacy behavior: self-disclosure and privacy-protective measures (e.g., being careful for groups joining and accepting friends' request, employing privacy settings). Four dimensions have been analyzed in terms of information privacy: collection, improper access, errors, and unauthorized secondary use. Participants were most worries about unauthorized access and lowered worried about selection among these measurements. From their research analysis, users who primarily used social networks online for entertainment or forming new relationships were similar to be concerned about several features of information confidentiality. Those who used the online social network to get information, alternatively, did not seem to be worried around privacy. These findings should be taken into consideration, given the poor interaction between two concepts and the weak prediction of all parameters of data privacy as a result of the reasons.

They discussed four different aspects of information privacy problems, so they may need to define alternate dimensions in the sense of online social networking sites for data privacy concerns. And from the Information Processing framework perspective [18], the aim of their research Mamonov and Benbunan-Fich [19] was to gain insight into the automatic responses of computer users to possible security and privacy risks.

They are based on the framework of data processing; threat mitigation usually occurs before an enhanced cognitive risk assessment. They performed experimental study to compare and contrast the impacts of public information security risks on two main user behaviors: the power of newly chosen passcodes and the reluctance to disclose personal information between two groups. In particular, they look at how much information users reveal about themselves and how strong the passwords they used to secure their answers after being exposed to many news reports about corporate computer security breaches. They came up with four hypotheses. They then performed an online experiment to test the hypotheses in their sample as a between-groups experiment.

Likewise, they discovered that participants in their study responded quickly to news reports about security and privacy violations by creating 500 stronger passwords and selectively restricting personal information disclosure. But, to obtain stronger behavioral responses, it might be necessary to find a more efficient way to present computer privacy and security messages.

After that, Zlatolas et al. [20] saw any ties among privacy concerns, trust, and online social networks information disclosure, particularly Facebook. It provided a model of how users' trust in online SNs, privacy concerns, privacy control, and self-disclosure on these platforms are influenced by the rate of confidentiality and perceived privacy risk. In their model, the concepts of privacy value and privacy risk are treated as separate constructs. Privacy risk is a notion that measures how users perceive their information is being used on Facebook, whereas Privacy value measures how users perceive their information is being protected on Facebook. According to their model, privacy risk influences Facebook trust and privacy concerns. The value of privacy affects privacy concerns. They also believe that Facebook trust affects self-disclosure, privacy concerns, and privacy control. This research provides six hypotheses, which

they collect data online questionnaires and samples in their study including Slovenian Facebook users.

The findings of the path analysis have confirmed five of the six test hypotheses. Both privacy value and privacy risk have a optimistic effect on privacy concerns, whereas privacy risk has a negative impression on Facebook trust. Self-disclosure, privacy concerns, and privacy control constructs all have an important outcome on the mediator constructing trust in Facebook. Furthermore, it was observed that trust in Facebook has a negative impact on one's willingness to disclose one's personal information on Facebook. However, they concentrated on Facebook members from Slovenia. As a result, this cannot be applied to all Facebook users in general. The search for and inclusion of potentially essential constructs relating to privacy, trust, and self-disclosure, such as a user's privacy awareness and behavioral intention, should be prioritized on online social networking sites.

The authors Jozani et al. [21] planned to study the effects of privacy concerns on both social and institutional levels of long-term behavior rather than the initial adoption on the user's appointment through social media applications inside the privacy calculus framework.

The authors assessed the benefits and costs of using social media-enabled applications. In particular, the framework for the privacy calculus is expanded by analyzing the distinct impact on user engagement of institutional and social privacy issues rather than one-time information expose actions, identifying distinguished experiences of these two privacy concerns, which include: (1) control, risk, and sensitivity of information (2) engagement (3) perceived benefits (4) control variables.

The discovery from 354 survey responses analysis indicates that engagement is diminished by both concerns in social and institutional privacy. About the antecedents, institutional privacy concerns are enhanced by the perceived information sensitivity. Nevertheless, A person's perspective of danger and control has an impact on their concerns about social privacy. More importantly, even while the outcomes of social and enjoyment benefits are expected to be favorable, the perception of operational efficiencies has the effect of decreasing involvement. Other antecedents, such as trust, accessibility, and self-efficacy, can be explored in researching elements that are relevant to private calculus in the case of social mobile devices in order to increase the strength of this study.

In another way, in their study of Li et al. [22], they indicated that they wanted to identify the users who carry the target users' private data rather than all the surrounding users. They attempted to compile a comprehensive list of users' privacy ratings all over the entire social network. They also hope to create an accurate and unbiased assessment of the confidential status of social networking site users based on the various data that users have made public as well as the network environment in which they are placed, among other things.

When determining a user's privacy state, they advocated for a more inclusive PMoB (Privacy Measurement of Behavior) methodology that included more factors. In the first instance, they take into account the users' attribute information from their profile and the graph framework, as well as the users' friend associations. And, in order to assess the privacy status of the target user, they used the SimRank algorithm to identify a user group that had a significant correlation with the target user's privacy leakage. It is also suggested that the concept of behavioral intimacy be used in order to gather

user behavior characteristics. They also integrated structural similarities and behavioral features to accurately filter the user groups based on the target user's current private information in order to eliminate the redundant user from the system.

They solved the problem of timeliness. As shown in the experimentations, the proposed PMoB approach can remove redundant users speedily and efficiently by integrating structural similarity and behavioral features, thereby giving the target users more accurate privacy scores.

This proposed PMoB has many limitations, where the calculation steps were tedious, and the calculations of these various characteristics of behavior and attributes were independent, neglecting the hidden relationships between characteristics.

In the study conducted by the authors Ayaburi and Treku [23], they endeavored to examine how organizational integrity can lead to decreasing privacy concerns of individuals while increasing the trust based on the Facebook case. Based on the Facebook case, they propose a research model in which the apology's persuasiveness following a data leakage influences user confidence or overspill honesty across their conceptions of the level of synchronization between the apology words and the violating entity's actions.

They began their model evolution by investigating organizational Behavioral Integrity via the lens of social accounts and trust, and by examining how these two concepts are intertwined. When the model is run, the underlying impacts of a data breach are applied, including the loss of ownership and control of users' private information, which is a concern that is incorporated in their privacy worries. It was discovered that the hypotheses were based on four variables: behavioral integrity, persuasive penal social account (PA), privacy concerns (PC), and trust. After that, the hypotheses were empirically tested and the proposed model was evaluated, with data obtained through the use of a survey instrument. The component-based partial least squares (PLS) technique was also employed in this investigation in order to assess the psychometric properties of measuring scales and to test the research hypotheses proposed in the findings of this study. The PLS is an ideal strategy for this research since it is a component-based approach that focuses on data prediction and is well-suited for constructing exploratory models and theories.

They found that while behavioral integrity performs a crucial role in the apology's persuasiveness and trust as an interposing factor, it entirely bridges the gap between the persuading apologies and the users' privacy worries by acting as a middleman between the two. However, consumers' privacy concerns have little effect on their faith in social media in the traditional sense. This article is required since it has been argued that the timing of response plays a critical role in restoring trust [24], and hence it must examine the appropriate timing of an apology and its efficacy in restoring trust. In addition to some recent investigations, such as those in [25–28].

4 Discussion

After the most relevant literature reviews in this field were presented in the previous section also defects and gaps were identified for each research paper; Table 1 summarizes this literature in terms of describing the research paper and the most important criticisms against it.

Table 1. Summary of related literature

Paper	Description	Critique
Wu et al. (2012) [9]	They showed how cross-cultural factors are considered, the content of confidentiality influences trust and privacy concerns, including the willingness to provide personal information online.	– Need to investigate the impact of gender and age. – Look at other factors that have an important outcome on trust and privacy.
Taddei and Contena (2013) [11]	They examined the relations between privacy, trust and control of explication for the publication of personal information in online SNs.	– The descriptions for the studied variables are still under debate.
Xu et al. (2013) [12]	They identified the main issues that effects on users' personal information self-disclosure. Incorporating the perceived advantage into the Planned behavior Theory was accomplished through the use of privacy calculus, and an integrated framework was explicitly proposed, with minor modifications for the setting of social networking sites.	– Could find other variables that have an effect on people's behavior choices. – Generalization of the study is restricted to a Chinese university student.
Zlatolas et al. (2015) [13]	To gain a well considerate of how confidentiality topics influence self-disclosure, they created a model that included the following constructs: privacy social norms, awareness of privacy, privacy control, privacy policy, privacy concerns, privacy value, and self-disclosure.	– Cannot be useful to all Facebook users worldwide. – Need to look for and include potentially important constructs related to privacy and self-disclosure.
Malik et al. (2016) [14]	They looked into the effects of several features of privacy correlated with photo sharing on Facebook.	– Can address constructs the user's privacy-related attitudes, expectations, and behaviors may be added to the measurement model. – The study was limited to only one social networking site, Facebook.
Chang et al. (2017) [15]	They contrasted LinkedIn and Facebook with the purpose of better understand the features that influence users' trust in social networking services.	– Emphasis was placed on two social networks categories (LinkedIn and Facebook), where another kind of social networks has different characteristics of user groups.
Aghasian et al. (2018) [16]	They suggested a new way to improve privacy in friending, they named the proposed: privacy-enhanced friending framework.	– It is possible to consider measuring users' knowledge around privacy.
Heravi et al. (2018) [17]	They sought to examine whether there is a contradiction between confidentiality concern and privacy behavior.	– Need defining alternate dimensions in the sense of online social networks for information privacy concerns.

(Continued)

Table 1. Summary of related literature *(Continued)*

Paper	Description	Critique
Mamonov and Benbunan-Fich (2018) [19]	This research team conducted an experimental investigation in order to determine the impacts and differences of an exposure to broad threats to information security on two major user behaviors.	– To obtain stronger behavioral responses, it might be necessary to find a more efficient way to present computer privacy and security messages.
Zlatolas et al. (2019) [20]	They saw if there were any ties between confidentiality concerns, trust, and online social networks information disclosure, particularly Facebook.	– Generalization of the study is restricted to Slovenian Facebook users. – Depend only on one social networking site, Facebook. – Can include potentially important constructs such as the privacy awareness and behavioral intention of users.
Jozani et al. (2020) [21]	They inspected the properties of both social and concerns about institutional privacy of long-term behavior rather than the initial adoption on the user's engagement with social media applications within privacy calculus framework.	– It contributes to the body of knowledge regarding mobile apps' privacy by investigating the impacts of institutional-al and social private information on customer engagement, as well as the various antecedents of these two forms of privacy issues. – To improve the strength, other factors such as trust, usability, and self-efficacy might be addressed in this survey when investigating elements that are essential to privacy calculus in the case of social mobile technology.
Li et al. (2020) [22]	They wanted to identify the users who carry the target users' private data, rather than all the surrounding users. They tried to collect users' privacy scores across the entire social network.	– PMoB has many limitations, where the calculation steps were tedious and the calculations of these various characteristics of behavior and attributes were independent, neglecting the hidden relationships between characteristics.
Ayaburi and Treku (2020) [23]	They endeavored to examine how organizational integrity can lead to decreasing privacy concerns of individuals while increasing the trust based on the Facebook case.	– Need to analyze the proper apology timing and its efficacy in rebuilding trust.

5 Limitations and future research directions

SNs carries risks that require awareness and caution when using them. Failure to act with caution may lead to revealing more details and information than necessary through pictures and personal information.

As a result, privacy has always been a major societal concern. This problem is turning increasingly critical as more people become involved in the digital world. Individuals are becoming increasingly worried about their privacy in the online world, as any move they take could drop a vestige of data that could be registered and used in the future. Therefore, identity privacy is one of the most important and sensitive issues, as its concerns lead to placing users at potential risk and thus lead to loss of trust.

Since there is a huge trend for social networks, there is a need to conduct extensive studies focusing on the user's long-term engagement with social networks over the Internet, which is the most important factor for preserving the privacy of identity instead of relying on the initial adoption of downloading and installing applications and adjusting settings. Where the user is the main factor in preserving privacy and therefore, there is a need for an approach that improves Protect identity privacy and builds trust in users' behavior on SNs.

Despite the fact that the concept of "self" manifests to be essential to privacy research, there are remarkably few studies that look at the relationship between psychological selfhood and the privacy of information. Also, in terms of issues of trust and privacy, the potential constructs impacting user behavior still need to be investigated further. Since trust is closely related to privacy, trust becomes an essential component of a successful social network. Therefore, we need studies that also focus on ways to enhance trust in social networks.

6 Conclusion

The SNs are a double-edged weapon, an entry point for many useful things. Still, unfortunately, it opens the way for many harmful things such as getting unwarranted access to personal information and can be used illegally. The goal of this research paper is to present the most important literature related to social networks in terms of privacy and trust, how they affect user behavior in these social networks, and what are the important methods and concepts they followed in protecting individual privacy and enhancing trust in user behavior and discussing them and what are the gaps that need to focus them in the future.

7 References

[1] Statista. Number of social network users worldwide from 2017 to 2025. [2020 Accessed 19 April 2021]; Available from: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[2] Sedikides, C., and Brewer, M. B. (2015). Individual self, relational self, collective self. Psychology Press. https://doi.org/10.4324/9781315783024

[3] Vignoles, V. L., Schwartz, S. J., and Luyckx, K. (2011). Introduction: Toward an integrative view of identity. In Handbook of identity theory and research Springer, New York, NY., pp. 1–27. https://doi.org/10.1007/978-1-4419-7988-9_1

[4] Smith, H. J., T. Dinev, and Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, p. 989–1015. https://doi.org/10.2307/41409970

[5] Sherchan, W., S. Nepal, and Paris, C. (2013). A survey of trust in social networks. ACM Computing Surveys (CSUR), 45(4): p. 1–33. https://doi.org/10.1145/2501654.2501661
[6] DataReportal. Global Social Media Stats. [2021 Accessed 28 August 2021]; Available from: https://datareportal.com/social-media-users
[7] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., and Prisma Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7): e1000097. https://doi.org/10.1371/journal.pmed.1000097
[8] Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33: p. 1–26.
[9] Wu, K.-W., et al. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 28(3): p. 889–897. https://doi.org/10.1016/j.chb.2011.12.008
[10] Liu, C., et al. (2004). Beyond concern: A privacy–trust–behavioral intention model of electronic commerce. Information & Management, 42(1): p. 127–142. https://doi.org/10.1016/j.im.2004.01.002
[11] Shaikh, A. (2015). NoMadCar: The interactive design using human computer interaction techniques. Journal of Advanced Computer Science and Technology Research, 5(1): p. 1–15.
[12] Xu, F., Michael, K. and Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. Electronic Commerce Research, 13(2): p. 151–168. https://doi.org/10.1007/s10660-013-9111-6
[13] Zlatolas, L. N., et al. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45: p. 158–167. https://doi.org/10.1016/j.chb.2014.12.012
[14] Malik, A., et al. (2016). Impact of privacy, trust and user activity on intentions to share Facebook photos. Journal of Information, Communication and Ethics in Society. https://doi.org/10.1108/JICES-06-2015-0022
[15] Chang, S. E., Liu, A. Y. and Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. Computers in Human Behavior, 69: p. 207–217. https://doi.org/10.1016/j.chb.2016.12.013
[16] Aghasian, E., Garg, S., and Montgomery, J. (2018). A privacy-enhanced friending approach for users on multiple online social networks. Computers, 7(3): p. 42. https://doi.org/10.3390/computers7030042
[17] Heravi, A., Mubarak, S., and Choo, K. K. R. (2018). Information privacy in online social networks: Uses and gratification perspective. Computers in Human Behavior, 84: p. 441–459. https://doi.org/10.1016/j.chb.2018.03.016
[18] Beck, A. T. and Clark, D. A. (1997). An information processing model of anxiety: Automatic and strategic processes. Behaviour Research and Therapy, 35(1): p. 49–58. https://doi.org/10.1016/S0005-7967(96)00069-1
[19] Mamonov, S. and Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior, 83: p. 32–44. https://doi.org/10.1016/j.chb.2018.01.028
[20] Nemec Zlatolas, L., et al. (2019). A model of perception of privacy, trust, and self-disclosure on online social networks. Entropy, 21(8): p. 772. https://doi.org/10.3390/e21080772
[21] Jozani, M., et al. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Computers in Human Behavior, 107: p. 106260. https://doi.org/10.1016/j.chb.2020.106260
[22] Li, X., et al., Using user behavior to measure privacy on online social networks. IEEE Access, 2020. 8: p. 108387–108401. https://doi.org/10.1109/ACCESS.2020.3000780

[23] Ayaburi, E. W. and Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. International Journal of Information Management, 50: p. 171–181. https://doi.org/10.1016/j.ijinfomgt.2019.05.014

[24] Gillespie, N. and Dietz, G. (2009). Trust repair after an organization-level failure. Academy of Management Review, 34(1): p. 127–145. https://doi.org/10.5465/amr.2009.35713319

[25] Contreras Espinoza, R. S., Blanco Martínez, A., and Eguía Gómez, J. L. (2021). Implementation barriers to augmented reality technology in public services. International Journal of Interactive Mobile Technologies (iJIM), 15: p. 43–56. https://doi.org/10.3991/ijim.v15i13.22667

[26] Hasan, R., Palaniappan, S., Mahmood, S., Sarker, K. U., Sattar, M. U., Abbas, A., and Rajegowda, P. M. (2021). eDify: Enhancing teaching and learning process by using video streaming server. International Journal of Interactive Mobile Technologies (iJIM), 15(11): p. 49–65. https://doi.org/10.3991/ijim.v15i11.20245

[27] Saeed, S., Shaikh, A., and Memon, M. A. (2018). Impact of social networking sites on personality & attitude of young adults (Research covering the young adults lives within Korangi, Karachi). International Research Journal of Arts & Humanities (IRJAH), 46(46).

[28] Awwad, A. M. A. (2021). Visual emotion-aware cloud localization user experience framework based on mobile location services. International Journal of Interactive Mobile Technologies (iJIM), 15(14): p. 140–156. https://doi.org/10.3991/ijim.v15i14.20061

8 Authors

Razan Saleh Almogbel, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia. E-mail: 411200003@qu.edu.sa.

Ali Abddulaziz Alkhalifah, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia. E-mail: a.alkhalifah@qu.edu.sa.

Article submitted 2021-10-25. Resubmitted 2021-12-13. Final acceptance 2021-12-14. Final version published as submitted by the authors.