PRINT ISSN: 2519-9781

ONLINE ISSN: 2710-1320

Understanding Security and Privacy Protection Measure Use in SNSs: A Systematic Literature Review

Dr. Abdulkadir Jeilani

Lecturer, Faculty of Computer Science and Information Technology, Mogadishu University

Email : a.jeilani@mu.edu.so

Orcid https://orcid.org/0000-0003-1995-1503

DOI: 10.1119/MUJ.2023718515

Abstract

Social networking sites have emerged as significant sources of internet traffic, capturing the attention of scholars across various disciplines. In the realm of information security, the discourse surrounding security and privacy on these platforms has gained substantial prominence. However, there has been a dearth of comprehensive reviews encompassing the current state of research and providing valuable insights into previous findings. This study aims to address this gap by conducting a systematic literature review to examine

the primary factors that influence users in their utilization or modification of security and privacy settings in social networking sites. The research data comprises 38 articles published between 2012 and 2022, sourced from diverse research databases including Mendeley, Google Scholar, and ScienceDirect. The analysis and synthesis of the field's status were performed using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines. The findings reveal that users' decisions to modify their security and privacy settings are predominantly influenced by factors such as concerns about information privacy, perceived awareness, trust, perceived severity of attacks, vulnerability, and perceived fear. The study also discusses the limitations encountered during the research process and proposes potential avenues for future investigation

Keywords: Security and Privacy Protection Measure, SNS, Systematic, Literature Review.

Introduction

The first generation of internet services for websites was Web 1.0 which is read – only web or static web sites and personal sites, the second is Web 2.0 referred participative social web or read – write web is the era (2000 and continues even now) the growth of social networking sites has been phenomenal, with Facebook, TikTok, Twitter and others emerging as prominent examples. The third generation of internet services for websites and applications is Web 3.0 that will focus on using a machine-based understanding of data to provide a data-driven and Semantic Web, this generation refers read, write and execute web. The social media has

been changed the way people communicate previous and make it easy people to communicate each other. According to some study(key,) as of January 2014, 74% of users who have access to the internet are also members of some OSNs. As a result, OSNs have become a part of peoples' daily life and a promising mechanism for people to connect to and interact with friends, colleagues and relatives [Pagoto etal.,2014] OSNs can even help users to reconnect with old friends who have long been lost in contact. A study conducted by (Ansari & Khan, 2020) more than two to third of social media users reported having one or more social networking site accounts.

Social networking websites have become platforms for cybercriminals for cybercrime; cybercriminals exploit sensitive and personal information through social engineering and reverse social engineering. It is usual for the users of social websites to share information; however, they lose privacy, while sharing information with strangers, they can fall in honey trap made by them. Privacy has become an important concern in online social networking sites. Users are unaware of the privacy risks involved when they share their sensitive information on the social network sites(Bender et al., 2017; Fire et al., 2014).

The default settings share everything, users have to change their default privacy setting options to make their accounts and personal information more secure. Security attacks continue to be a major concern of all users. How to keep social networking sites more secure and more private are the challenges that have been concern for every user.

For many users of online social networking websites, there are two ways for them to protect their data. The first, of course, is to refrain from making the item available online. This is not a viable option, given that the purpose of online social networks (OSN) is to share information and communicate with others. The second option is to use the privacy controls provided to manage who can see which items. While the second option appears viable, both formal studies and anecdotal evidence suggest that configuring privacy policies and managing access control policies is a difficult task for most users(Madejski et al., 2012). It is difficult for social networking sites and users to make and adjust privacy setting to protect privacy without practical and effective way to identify measure and evaluate privacy. Maximum numbers of users are not aware of the security risk associated whenever they shared sensitive data on the social sites, so that privacy concern will be raised among those online communications if their personal data has been shared to other users. The users should be aware of their privacy quotient and should know where they stand in the privacy measuring scale. Unfortunately, many users are not aware of this and become victim of privacy and identity breach (Roshan Jabee, M. A. Alam, 2016).

The literature is filled with studies on information sharing, privacy paradox and self-disclosure(Hazari & Brown, 2013; Kante & Michel, 2023) but little attention is devoted to explain the Security and Privacy Protection Measure Use in SNSs. The users' situation due to privacy concerns is utmost challenge for their trust of social media platform but the users still use social media despite their concerns over. In addition, a systematic review of previous studies is needed to synthesize previous

findings, identify gaps that need more research, and provide opportunities for further research. The aim of this study is to explore the current literature in order to understand security and privacy measure in social networking sites. In order to achieve effective results in a clear and understandable manner, two research questions were proposed as shown below.

(1) What are the key factors that effects users to change their security and privacy settings on social networking sites?

(2) What were the major theories adopted in previous studies on security and privacy protection measure use in SNSs?

Method

The aim of this study is to perform a systematic literature review for identifying the key factors that effects users to change their security and privacy settings on social networking sites and theories adopted by each paper. The research employed the PRISMA method to ensure that a rigorous and efficient review process was done, we have followed the guidelines of the updated Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) 2020 statement (Page et al., 2021) to conduct this study. The PRISMA 2020 for Abstracts and items Checklist can be found in the appendix of this paper. The PRISMA guidelines have been largely used and endorsed, as evidenced by its co-publication in multiple journals, citation in more than 60,000 reports with endorsement from almost 200 journals and systematic review organizations, and adoption in various disciplines as well(Page et al., 2021). The below figure is the PRISMA flow chart.

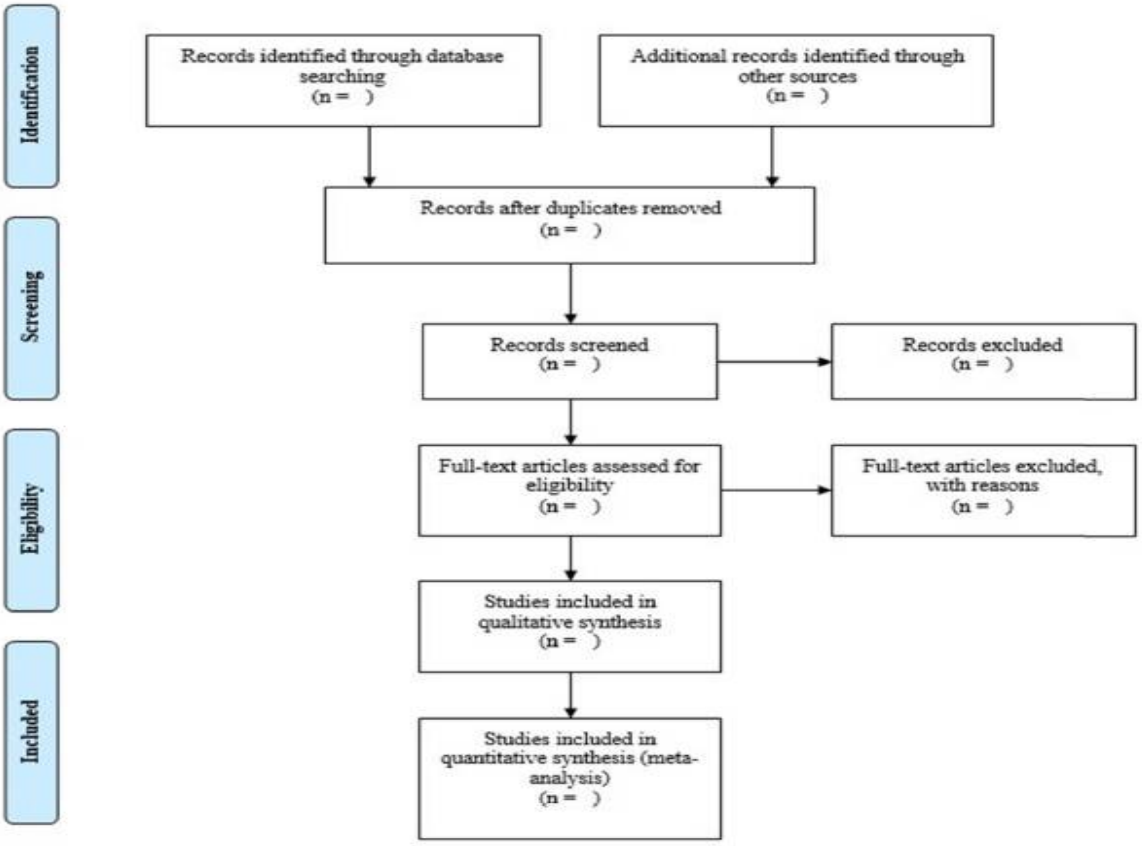

Fig. 1. The PRISMA flow diagram.

Research questions

In this study, the researchers aimed to answer the following research questions:

Table1. Research questions

SLR research question	Rational and motivation
RQ2. What are the key factors that effects users to change their security and privacy settings on social networking sites?	This question aims to identify the factors that influencing users to modify their security and privacy settings in social networking sites. This will increase to focus of each social media of security and privacy options or protection measure.

SLR research question	Rational and motivation
RQ1. What were the major theories adopted in previous studies on security and privacy protection measure use in SNSs?	The answer of this question will allow us to detect what kind of theories used in the previous studies. These theories provide a theoretical foundation of the student privacy protection behavioral in social networking sites(SNSs)

Data source

The researchers developed search strategy and tailored to eight large databases: ACM Digital Library, EBSCO, Google scholar, Science Direct, Springer Link, IEEE Xplore, IGI Global, Web of Science, PsycINFO and Scopus and the search items used were the following: security and privacy settings in social media all searches spanned from databases inception until 2023.

Quality assessment

For maintaining the quality of the review all duplications were checked thoroughly. Abstract of the articles were checked deeply for the analysis and purification of the articles to ensure the quality and relevance of academic literature included in review process.

Data extraction

Once the researchers assessed the quality of the data, data was manually extracted from the research papers as the table below shows. List of Data Extraction Template

1. Author
2. Title
3. Year publication
4. Reference
5. Study research area
6. Methodology [Case study, Survey, Systematic literature review]
7. Research objectives / purpose
8. Country
9. Sample size
10. Type of sample
11. Data analysis [Qualitative, Quantitative, Mixed and Thematic analysis]
12. Data collection [interview, questionnaire, focus group, observation and discussion etc]
13. Study results and conclusion
14. Type of article [Journal, conference, technical report]
15. Key factors that influence users to change security and privacy settings on social networking sites
16. Theory adapted in each study

Tools and Analysis

The researchers used Mendeley desktop and MS Excel spreadsheet as a tool for data management and data analysis. Mendeley permits storing papers and managing them appropriately by providing tools to tag,

classify, and reference papers using various attributes. Moreover, the item extracted were stored and used to clean the data and make descriptive statistics using Microsoft Office Excel. The current study reviewed 35 research papers. The selection process has been summarized in the figure 2. To identify literature pertinent to security and privacy settings on social networking sites. For article to be included in our systematic review, it must have a focus on privacy measures on social media. The databases and search engines we found 582 records; 91 records were eliminating as they were not related to our searching keywords special in the titles and abstracts. The full text of the remaining 491 were carefully screened and 285 were excluded, as they did not meet the selection criteria. Other records were included by the looking the following criteria Study does not address primary endpoint (n=100), Full texts cannot be accessed (n=50), Report, Review, Systematic review and meta-analysis (n=38)

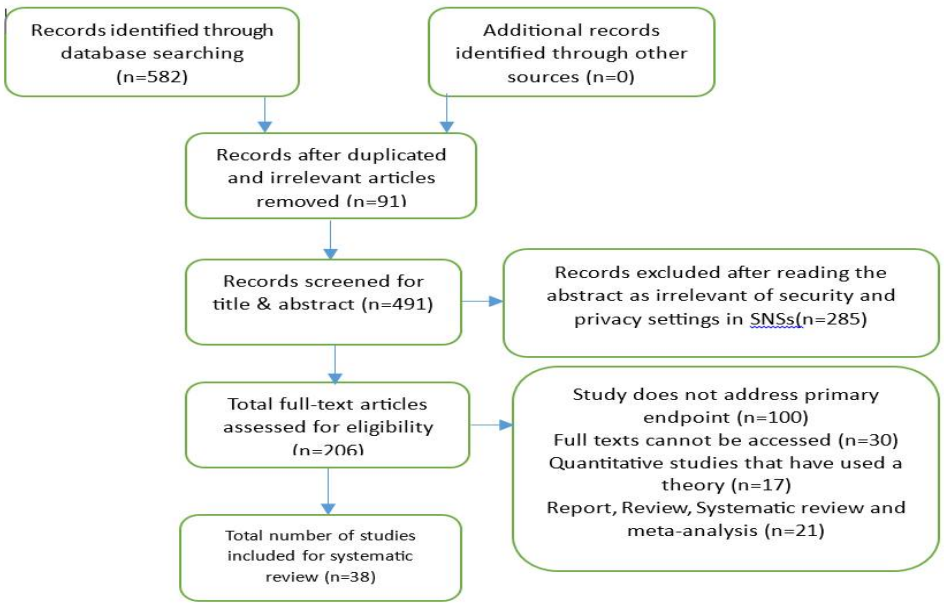

Fig2. Flow diagram search

Selection criteria

This systematic review was conducted by following the reporting checklist of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA; Liberati et al. 2009). The purpose of the study was undertaken a comprehensive literature search to identify security and privacy settings in social networking sites and included all the papers published in English only and papers published until June 2023. All The selection criteria were based on the PRISMA statement(Rethlefsen et al., 2021). The search mainly focused on the mapping existing literature on security and privacy settings in social networking sites in the field of general Information System, Computer Science, Computer Applications, Computer Vision and Pattern Recognition, Computer Networks and Communications, Human – Computer Interaction. The search then narrowed to the subject areas to information security, Computer Networks and Communications, cybersecurity, security and privacy. The last search was run on 2st July 2023.

The title, abstract, keywords, authors' names and affiliations, journal name, and year of publication of the identified records were exported to an MS Excel spreadsheet. The researchers screened the titles and abstract of the records and discarded the papers like systematic review, research reports and meta – analysis and included journals articles such as empirical, descriptive and conceptual papers. The search span was from year 2012 – 2023. All articles before 2012 were excluded from search. The researchers were focused the content of each study using three selection criteria: (1) focus on security and privacy settings or options;(2)

an investigation of the context of social networking sites, social media or online social networks; (3) and a qualification an empirical study. After applying these criteria, a total of.

The researchers investigated the reference lists of all received articles to identify any additional studies that was not included our database search. In total, the researcher observed the 41 published across 40 academic journals and 2 unpublished manuscripts on security and privacy measure in social networking sites from 2010 to July 2023 inclusive with in the sample, there were 38 quantitative research papers, and 2 qualitative papers. In analyzing the trends in these publications, we can see that 2018 was the most published quantitative research papers related to the security and privacy concern on social media.

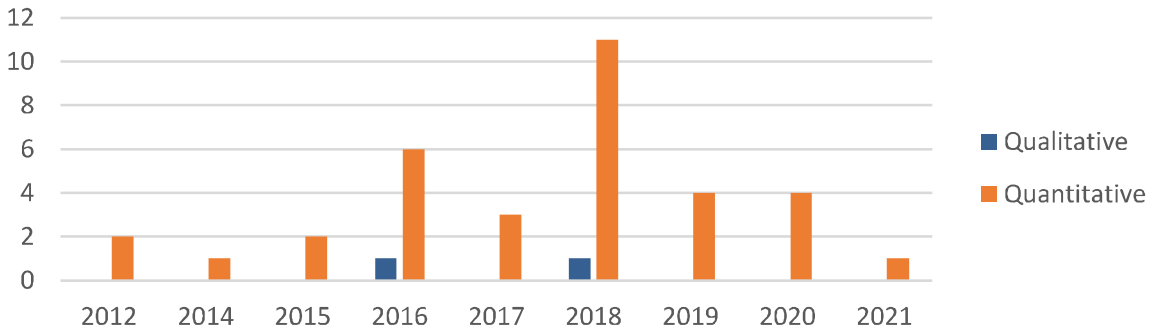

Fig3. Security and privacy measure publications by year and study type

Since 2010, studies on security and privacy measure in social networking sites has increasingly been published in the high impact factor journals, including Computers in Human Behavior, Behaviour & Information Technology, Computers & Security, and new media &

society. The below the table indicates the number of journals that at least published two to more articles.

Table 2. Journals at least 2 to more articles

Journal	No of articles	Impact factor	Source
Computers in Human Behavior	7	9.9	Elsevier Ltd
Behaviour & Information Technology	4	0.6	Taylor & Francis
Computers & Security	3	5.6	Elsevier Ltd
new media & society	3	5.0	Sage Journals
Social Media + Society	2	2.04	Sage Journals

Results

The current study reviewed and analyzed the 35 studies to answer our research questions which are: (1) What are the key factors that effects users to change their security and privacy settings on social networking sites? (2) What are the theoretical and empirical studies, have effect actual use of security and privacy protection measures on social networking sites and what are the most accepted ones theoretically?

Q1. What are the most factors that influence users to use security and privacy protection measure in social networking sites through theoretical and empirical studies?

Although a long range of benefits that can be obtained from using social networking sites but many individuals have privacy concerns. Report according to academic experts, professional and social media

providers related to security and privacy on social media almost 75% concern information privacy are important factors in their decision to change their settings on social networking sites. Fear appeal, self-efficacy, fear, and response efficacy were found to have a positive impact on users' adoption of privacy security measures(Zhu et al., 2020). Dhami et al.(2013)found that privacy concerns, such as security and trust, have a positive effect on information sharing. Salleh et al.(2013) also found that trust on social networking sites and perceived benefits influenced information disclosure behavior. However, perceived privacy risk did not have a significant impact on self-disclosure. Shin (2010)found that perceived security and privacy were distinct constructs that influenced users' trust and intention to use social networking sites. Gupta & Dhami (2015) also found that users' behavioral intention to share information on social networking sites was influenced by their perceptions of security, trust, and privacy. Hoffmann (2012)found that users who believed security was important were more likely to change their security settings, and users who set their privacy to a custom setting were less likely to receive an attack on their profile. Barrett-Maitland et al. (2016)found that privacy and security controls were fundamental values for users in maximizing their security and privacy on social networking sites. Ho et al. (2009)found that users are not properly informed of the risks associated with using social networking sites and applications, and that the privacy settings provided by these sites are not flexible enough to protect user data. Krasnova (2009) found that users' privacy concerns can lead to reduced network activities and self-disclosure, which can negatively impact network sustainability and business value. Schaik et

al.(2018)found that users who do not regulate their information-sharing on social networking sites face the highest perceived risk and dread, and that users who take precautionary measures tend to have higher perceived control and Internet experience. Overall, the papers suggest that users who do not use the security and privacy settings in social networking sites face potential risks to their privacy and security, and that network providers may need to develop specific mechanisms to alleviate user concerns and ensure network sustainability. Gupta & Dhami (2015) emphasizes the need for an exploratory study into users' behavioral intention to share information, as online interaction and sharing of personal information on social networking sites has raised new privacy concern. Foltz et al.(2016)found that attitude, subjective norm, and perceived behavioral control predicted behavioral intention, which in turn positively influenced behavior.

Awareness, trust and training are other factors may affect users to change their privacy settings on social media. Kim & Ammeter (2014) found that security function awareness and information security awareness are important antecedents for intention to use security functions. Shin (2010) proposed an SNS acceptance model that integrates cognitive and affective attitudes, driven by underlying beliefs, perceived security, perceived privacy, trust, attitude, and intention. Maitland (2013) applied the Value-focused Thinking (VFT) methodology to determine users' values and objectives, finding that privacy, confidentiality, integrity of SNS, security controls, awareness campaigns, corporate social responsibility, and personal responsibility are fundamental values in maximizing user security and privacy

conditions. Mousavi (2020) proposed a conceptual model that explains SNS users' privacy protection behavior based on protection motivation theory, finding that users' coping appraisals of the overall SNS assurance mechanisms, along with their threat appraisals, positively relate to their protection motivation. Increasing risk awareness and knowledge, as well as addressing protection obstacles, can support users in protecting their digital privacy Gerber (2020). Privacy concerns, perceived threat, perceived anonymity, perceived intrusiveness, perceived severity, self-efficacy, perceived vulnerability, and response efficacy (Suhaimi, 2020; Fujs, 2019; Khatri, 2021; and Namara ,2021). Overall, users' awareness of security and privacy issues, perceived threats, perceived anonymity trust in SNS providers, and perceived effectiveness of security and privacy measures are important factors in their use of security and privacy settings in SNSs. The below table depict the research topics and major factors contribute users to change their security and privacy settings.

Table 3. Biometric overview of the selected papers

No	Titles	Factors	References
1	Determinants of Privacy Protection Behavior in Social Networking Site	Perceived severity, perceived vulnerability, self-efficacy, response efficacy, perceived anonymity and Privacy Protection Bevahior	Siti Norlyana Suhaimi, Nur Fadzilah Othman, Raihana Syahirah Syarulnaziah Anawar, Zakiah Ayop, Cik Feresa Mohd Foozy (2020)
2	Everybody wants some: Collection and control of personal information, privacy concerns, and social media use	Personal information, privacy, privacy paradox, social media, social media enthusiasm, terms of service	Jason Anthony Cain and Iveta Imre(2022)

No	Titles	Factors	References
3	Privacy concerns on social networking sites: Interplay among posting types, content,and audiences	Privacy concerns on social networking sites (SNS) Content shared on social media Posting types	Yongick Jeong, Yeuseung Kim (2017)
4	Perceived vulnerability of cyberbullying on social networking sites: effects of security measures, addiction and self-disclosure	Use security measures, website security measure, voluntary self-disclose, addition, perceived vulnerability	Shilpi Jain,Soni Agrawal(2020)
5	Predicting users' privacy boundary management	Online privacy; privacy boundary; Facebook; self-disclosure; Facebook usage	Qian Liu, Mike Z. Yao, Ming Yang & Caixie Tu (2017)
6	strategies on Facebook	Privacy concerns, awareness, Personal attributes	
7	A survey of social meida users privacy settings & information disclosure	Information security awareness, perceived privacy control, privacy concerns	Mashael Aljohan, Alastair Nisbet, Kelly Blincoe(2016)
8	Social media privacy management strategies: A SEM analysis of user privacy behaviors	information security awareness, perceived privacy control, privacy concerns,	Kuo-Cheng Chung a, Chun-Hung Chen a, Hsueh-Hsuan Tsai a, Ya-Hsueh Chuang (2021)
9	Motivational Factors in Privacy Protection Behaviour Model for Social Networking Sites	perceived severity, perceived vulnerability, response efficacy and self-efficacy towards information privacy concern, privacy protection behaviour strategies	Muliati Sedek1, Rabiah Ahmad2, and Nur Fadzilah Othman(2018)
10	Relative Importance of Determinants Towards Users' Privacy Disclosure on Social Network Sites by	Motivational factors, Situational Factors, Rational Factors	L. T. Huang, J. D. Leu2(2020)

No	Titles	Factors	References
	Privacy Invasion Experience Based on Construal Level Theory		
11	Digital nudging and privacy: improving decisions about self-disclosure in social networks	perceived control, trust in provider and perceived privacy risk	Tobias Kroll & Stefan Stieglitz (2019)
12	Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory	perceived privacy risk and modelled severity and vulnerability as antecedents to perceived privacy risk. Trust, privacy value, and awareness were also measured as privacy risk antecedents	Tziporah Stern*; Nanda Kumar(2017)
13	Examining privacy settings on online social networks: a protection motivation perspective	Narcissism and self-esteem can explain tendencies to control privacy on two widely used platforms: Instagram and Twitter	Yioryos Nardis & Elliot Panek(2018)
14	Explaining Privacy Control on Instagram and Twitter: The Roles of Narcissism and Self-Esteem	perceived use of privacy policies and management features, among social networks' users,	Mohd Ishak Ismail1, Md Arafatur Rahman1, 2 and Saiful Azad(2016)
15	Exploiting Privacy-Policy and -Management Features on Social Networks: A User's Perspective	Online privacy concerns, privacy beliefs. Trust.	Mary Helen Millham and David Atkin (2018)
16	Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors	privacy concerns, personal information, self-presentational information	Jinyoung Min(2016)

No	Titles	Factors	References
17	Personal Information Concerns and Provision in Social Network Sites: Interplay Between Secure Preservation and True Presentation	Behavior, Trust, Policies, Technology	Sunil Hazari & Cheryl Brown(2014)
18	An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites	the configuration behavior of the privacy settings, (2) the deviation from the default option, and (3) the size of deviation from the default option.	Markus Tschersich(2015)
19	Comparing the Configuration of Privacy Settings on Social Network Sites Based on Different Default Options	privacy invasion experience enhances perceived personal risks, but website reputation helps to reduce perceived risks.	Kai Li,Xiaowen Wang,Kunrong Li,Jianguo Che(2016)
20	Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia	perceived severity, self-efficacy, perceived vulnerability, and gender were found to be ante-cedents of information privacy concerns in social networking sites	Mohamed, Norshidah Ahmad, Ili Hawa(2012)
21	Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective	privacy awareness, privacy concerns, and privacy invasion experience to be significant predictors of self-disclosure	George Oppong Appiagyei Ampong 1 Aseda Mensah 2,*, Adolph Sedem Yaw Adu 3, John Agyekum Addae 4, Osaretin Kayode Omoregie 5 and Kwame Simpe Ofori(2018)
22	An empirical study	Privacy concern, SNS fatigue,	Xinhua Zhu;Zheshi Bao(2018)

No	Titles	Factors	References
	integrating impression management concern, privacy concern, and SNS fatigue	SNS, Impression management concern, Passive SNS use	
23	Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks	Information privacy concerns; privacy protection; protection motivation theory; social cognitive theory; social networks	Adhikari, Kishalay Panda, Rajeev Kumar(2018)
24	Security and privacy in online social networking: Risk perceptions and precautionary behaviour	Online privacy Information security social media Risk perception Facebook Precautionary behaviour	Paul van Schaik a, Jurjen Jansen b, Joseph Onibokun, Jean Camp, Petko Kuseve(2018)
25	An Exploration of the Frequent Use of Social Networking Sites and Severity Attack among Undergraduate Students in Somalia	Social Networks, Online attacks, Perceived Attack, Vulnerability, Severity Attack, Protection Motivation Model.	Jeilani, Abdulkadir Kandiri, John M(2018)
26	Information privacy, consumer alienation, and lurking behavior in social networking sites	Information security awareness, Concern for information privacy, Consumer alienation, Privacy risk belief, Lurking, Self-concealment	Jaime Ortiz, Wen-Hai Chih, Faa-Shyan Tsai (2017)
27	Information Privacy in Online Social Networks: Uses and Gratification perspective	Information privacy concern was examined by four dimensions: collection, errors, improper access and unauthorized secondary use. Self-disclosure was examined through four dimensions:	Alireza Heravi, Sameera Mubarak, Kim-Kwang Raymond Choo(2018)

No	Titles	Factors	References
		amount, breadth, depth and honesty.	
28	Understanding online safety behaviors: A protection motivation theory perspective	Online safety; Computer security; Protection Motivation Theory; Response cost; Habit strength	Author: Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, Shelia R. Cotton(2016)
29	Personality, Attitudes, Social Influences, and Social Networking Site Usage Predicting Online Social Support	perceived ease of use, perceived usefulness, perceived enjoyment, attitude toward using SNS, and social influence to help understand social networking sites usage behaviors and online social support	Vikanda Pornsakulvanich PII(2017)
30	Effect of penitence on social media trust and privacy concerns: The case of Facebook	Apology Behavioral integrity, Privacy concerns Trust, Facebook, social media	Emmanuel W. Ayaburi, Daniel N. Treku(2020)
31	Privacy Management Among Social Media Natives: An Exploratory Study of Facebook and Snapchat	this study tested network size, network diversity, privacy concerns, and privacy management practices in and between Facebook and Snapchat for social media natives	Erin E. Hollenbaugh(2019)
32	Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on social media: Facebook, Twitter, and	Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on social media: Facebook, Twitter, and	Valentinus Paramarta, Muhammad Jihad, Ardhian Dharma, Ika Chandra Hapsari, Puspa Indahati Sandhyaduhita and Achmad Nizar

No	Titles	Factors	References
	Instagram	Instagram	Hidayanto(2018)
33	Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective	Privacy concerns, Privacy calculus, Engagement, social media-enabled apps, Social mobile era	Mohsen Jozani a, Emmanuel Ayaburi, Myung Ko a, Kim-Kwang Raymond Choo(2020)
34	Saving face on Facebook: privacy concerns, social benefits, and impression management	Impression management; privacy; social media; social exchange theory; trust	Jeffrey G. Proudfoot, David Wilson, Joseph S. Valacich & Michael D. Byrd(2017)
35	Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies	privacy, self-disclosure, disclosure management, social network sites	Philipp K. Masur and Michael Scharkow(2016)
36	Respondents view of novel framework for data protection in social networking sites: an analysis	Communication privacy management theory, online social networks, personal information, privacy	Mary Helen Millham and David Atkin(2018)
37	The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption	graphical authentication, watermarking feature, encryption technique, approval of friendship request	Shilpi Sharma(2019)
38	Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites	Self-disclosure; privacy; social network sites; digital nudging; persuasion	Tobias Kroll & Stefan Stieglitz(2019)

The figure below depicts the number of articles, conference papers and thesis published in the various countries between 2012 and 2021.

The figure also shows that the number of articles published in the countries have been relatively stable over the past decade, with a slight decline in recent years. The number of conference papers published has increased slightly over the same period. The number of theses published has decreased slightly over the past decade.

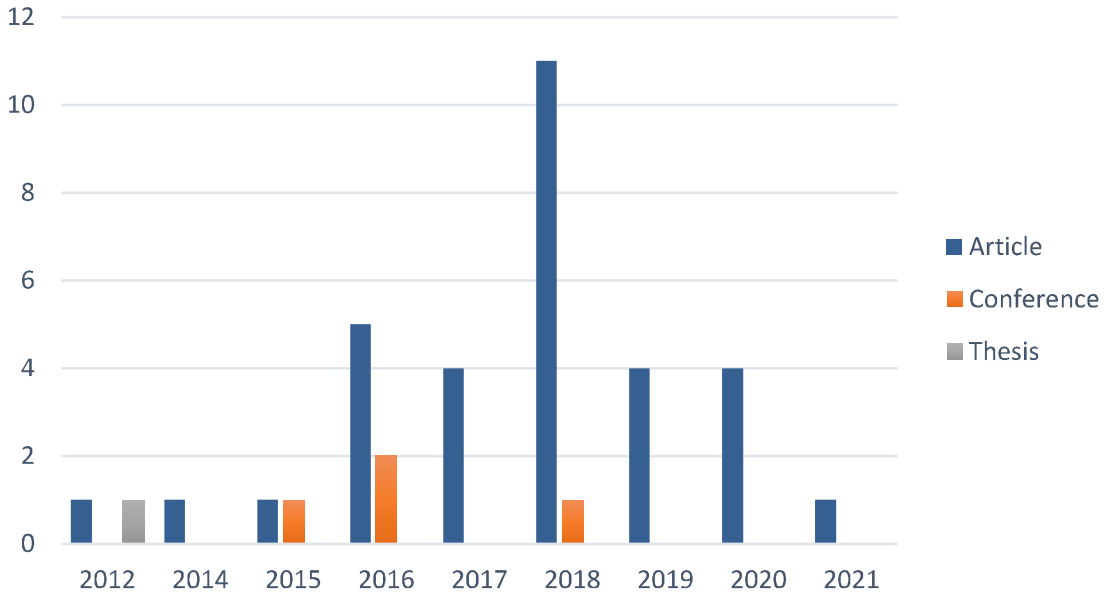

Fig4. Number of articles, conference papers and thesis

Q2: What were the major theories adopted in previous studies on security and privacy protection measure use in SNSs?

The results from the SLR show that previous studies used several theories to understand security and privacy protection measure use in social networking sites. Fig 3. depicts the theories used in these studies, with Protection Motivation Theory (PMT) being the most popular theory use to understand security and privacy protection measure use. Furthermore, Communication Privacy Management Theory (CPMT) and Privacy Calculus Theory (PCT) were second and third applied theories in

the studies. The theoretical insights into security and privacy measure use in social networking sites

Motivation aspect: since the emerge the privacy issues of social networking sites, many studies have been conducted to understand what motivates users to use security and privacy measure in social networking sites. Theories such as PMT, CPMT and PCT have been widely used to understand security and privacy issues. For instance, Suhaimi (2020) found that perceived anonymity, perceived intrusiveness, perceived severity, self-efficacy, perceived vulnerability, and response efficacy are significant determinants in motivating privacy behavior among high school students using the theoretical foundation of PMT. Baruh (2017) found that users concerned about privacy were more likely to utilize privacy protective measures. Khatri (2021) identified privacy and security issues in SNS and proposed a Privacy and Security Framework as a foundation to deal with these problems. Vivekanandam (2022) investigated the potential dangers of social networking sites and provided remedies to avoid them.

Privacy issues aspect: privacy issues are a major concern in social networking sites (SNS). Users share a lot of personal information on SNS, and there are many potential threats to data privacy and security, such as fraud, identity theft, and disclosure of sensitive information. The privacy settings provided by SNSs are not always flexible and reliable enough to protect user data, and users often lack control over what others reveal about them. Kim (2015) applies the Protection Motivation Theory to understand how assurance mechanisms affect users' self-disclosure

intention. Alqubaiti (2016) proposes that Protection Motivation Theory can be used to explain and predict users' behaviors that have security implication. Schneider (2021) explores the influence of Protection Motivation Theory (PMT) constructs on security behaviors of undergraduate students. Zhu et al. (2020)examines the influencing factors of APP Users' Privacy Protection Behavior based on the theory of fear appeals.

Information disclosure behavior: Krasnova (2011) and Krasnova (2010) both use the privacy calculus theory to study the differences in privacy perceptions and self-disclosure behavior between German and American social networking site users. They find that cultural differences impact self-disclosure and that social network providers need to adjust their strategies accordingly. Sipior (2013) applies an extended privacy calculus model to understand information disclosure behavior in online social networking and proposes a taxonomy of information integral to social networking sites. Wagner (2018) extends the privacy calculus theory by incorporating a social perspective and interpersonal communication theory to understand self-disclosure decisions on social networking sites. privacy calculus theory can be used to understand the complex decision-making processes involved in privacy issues in social networking sites.

Security and Privacy measure use: this study have recognized the Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Unified Theory of Acceptance and Use of Technology (UTAUT) were also utilized as

theoretical foundation in a number of primary studies. These theories have been widely applied in the information systems (IS) field to offer insights into information technology adoption among users(Zhang & Benyoucef, 2016). Users' behavior on social networking sites is influenced by various factors related to security and privacy measures. Kim & Kim (2020) found that perceived control over personal information plays a significant role in enhancing trust in SNS providers, users' intention to disclose personal information, and users' disclosing behaviors. Leng (2011) used the Technology Acceptance Model and Theory of Planned Behavior to explore factors that encourage students to adopt social networking sites in Malaysia, finding that perceived enjoyment is a more significant antecedent of attitude than perceived usefulness. Ho (2017) uses an extended theory of planned behavior (TPB) to explore how various factors, including personality traits, privacy concern, past privacy protection behaviors, and parental mediation strategies, relate to adolescents' intention to engage in privacy protection measures.

The below Fig 3. Depict the theories used in this study. Protection Motivation Theory were most widely used theory which is 29%, Communication Privacy Management Theory the secondly widely used (24%) and Privacy Calculus Theory (PCT) the third widely used (12%), 11% of the studies used Technology Acceptance Model (TAM), 8% of the studies applied Social Determination Theory (SDT). The remaining 5% Social Exchange Theory (SET), 4% Theory of Reasoned Action (TRA) similar Theory Planned Behavior (TPB) and 3% Uses Gratification Theory (UGT).

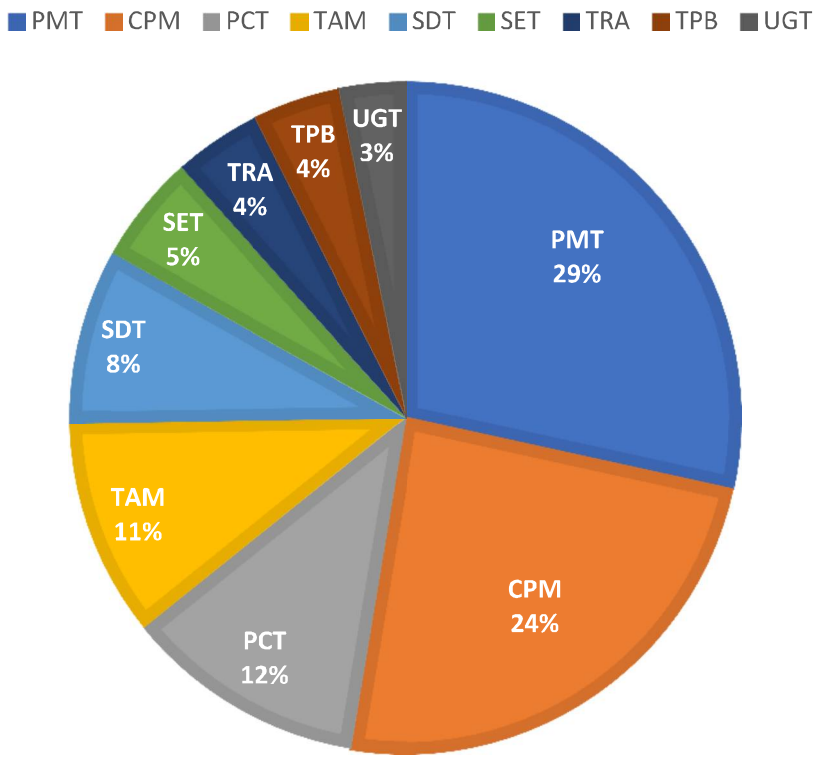

Fig5. Most of theories in selected papers

Conclusion and Future Agenda

Social networks play a crucial role as a major source of internet traffic, with 4.8 billion global users, representing 59.9% of the world's population and attracting over 92% of internet users worldwide. The growth of social networking sites continues, with 150 million new users joining in April 2023, reflecting a 3.2% year-over-year increase. While users have the power to control their privacy on these platforms, many are unaware of the risks associated with indiscriminate disclosure of personal information, despite notifications from platforms like Facebook. Although social media platforms offer advanced privacy control tools, they are often underutilized due to their lack of user-friendliness.

According to former Facebook CTO Bret Taylor, frequent Facebook users are highly conscious of privacy settings and take steps to protect their personal information. A significant majority (75.7%) of fixed internet users set their social media privacy settings to "friends only," while 20% allow visibility to anyone.

This study focuses on identifying and summarizing the main factors that influence users to utilize or modify their security and privacy settings on social networking sites. The research reveals that factors such as information privacy concern, perceived threat, anonymity, fear, intrusiveness, severity, self-efficacy, vulnerability, response alienation, privacy risk belief, lurking, self-concealment, information disclosure, intimacy, perceived effectiveness, and perceived training are significant contributors to users modifying their security and privacy settings. The study also highlights the predominant theories employed in previous research, including Protection Motivation Theory (PMT), Communication Privacy Management Theory (CPMT), Privacy Calculus Theory (PCT), Technology Acceptance Model (TAM), and Social Determination Theory (SDT), respectively.

The need for more user-friendly security and privacy measures in social networking sites is emphasized, as users often lack sufficient information to make informed decisions about their privacy. Future research should focus on the development of effective security and privacy measures while identifying research gaps for predicting the future of security and privacy in social networking sites.

Recommendations

Based on the findings of the study, the following recommendations are suggested:

1. Enhancing User Awareness: Social networking sites should prioritize educating users about the potential risks associated with disclosing private information. Efforts should be made to raise awareness about the importance of privacy protection and inform users about the available tools and settings to control their privacy.
2. Improving Usability of Privacy Settings: Social networking platforms should invest in designing user-friendly privacy settings that are easy to understand and navigate. This will encourage users to actively utilize and modify their security and privacy settings according to their preferences.
3. Strengthening Privacy Training: Providing comprehensive privacy training and resources to users can empower them to make more informed decisions regarding their privacy. Platforms should offer clear guidelines, tutorials, and support to help users effectively manage their privacy settings.
4. Addressing Perceived Threats: Social networking sites should actively address users' concerns regarding privacy threats. This can be achieved by implementing robust security measures, transparent data handling practices, and timely notifications about potential risks or breaches.

5. Incorporating Privacy-Enhancing Features: Platforms should continuously innovate and introduce new features that enhance user privacy, such as granular control over data sharing, encrypted communication, and privacy-preserving algorithms. These features should be regularly updated and communicated to users.
6. Collaboration with Researchers and Experts: Social networking sites should collaborate with researchers, privacy experts, and relevant stakeholders to continuously evaluate and improve their privacy measures. This collaboration can help identify emerging threats, explore effective strategies, and ensure ongoing privacy protection.
7. Engaging Users in Privacy Discussions: Platforms should actively involve users in privacy-related discussions, seeking their feedback and suggestions for improving privacy measures. This user-centric approach can foster a sense of ownership and trust, leading to more effective privacy protection.
8. Regulatory Compliance: Social networking sites should comply with relevant privacy laws and regulations, ensuring that user data is handled in a lawful and responsible manner. Regular audits and transparency reports can demonstrate their commitment to privacy protection.

Reference

Ansari, J. A. N., & Khan, N. A. (2020). Exploring the role of social media in collaborative learning the new domain of learning [Explorando el papel de las redes sociales en el aprendizaje colaborativo el nuevo dominio del aprendizaje]. *Smart Learning Environments*, *7*(1), 1–16. https://n9.cl/nju00

Barrett-Maitland, N., Barclay, C., & Osei-Bryson, K. M. (2016). Security in Social Networking Services: A Value-Focused Thinking Exploration in Understanding Users' Privacy and Security Concerns. *Information Technology for Development*, *22*(3), 464–486. https://doi.org/10.1080/02681102.2016.1173002

Bender, J. L., Cyr, A. B., Arbuckle, L., & Ferris, L. E. (2017). Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment. *Journal of Medical Internet Research*, *19*(4), e7029. https://doi.org/10.2196/jmir.7029

Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013*, 465–469. https://doi.org/10.1109/IADCC.2013.6514270

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys and Tutorials*, *16*(4), 2019–2036. https://doi.org/10.1109/COMST.2014.2321628

Foltz, B. B., Newkirk, H. E., & Schwager, P. H. (2016). An empirical investigation of factors that influence individual behavior toward changing social networking security settings. *Journal of Theoretical and Applied Electronic Commerce Research*, *11*(2), 2016–2017. https://doi.org/10.4067/S0718-18762016000200002

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites.

Journal of Direct, Data and Digital Marketing Practice, *17*(1), 43–53. https://doi.org/10.1057/DDDMP.2015.32/FIGURES/2

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. https://doi.org/10.1080/15536548.2013.10845689

Ho, A., Maiga, A., & Aïmeur, E. (2009). Privacy protection issues in social networking sites. *2009 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, 271–278. https://doi.org/10.1109/AICCSA.2009.5069336

Hoffmann, B. C. (2012). An exploratory study of a user's Facebook security and privacy settings. In *Theses, Dissertations, and Other Capstone Projects*. http://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=1069&context=etds

Kante, M., & Michel, B. (2023). Use of partial least squares structural equation modelling (PLS-SEM) in privacy and disclosure research on social network sites: A systematic review. *Computers in Human Behavior Reports*, *10*(September 2022), 100291. https://doi.org/10.1016/j.chbr.2023.100291

Kim, B., & Kim, D. (2020). Understanding the Key Antecedents of Users' Disclosing Behaviors on Social Networking Sites: The Privacy Paradox. *Sustainability 2020, Vol. 12, Page 5163*, *12*(12), 5163. https://doi.org/10.3390/SU12125163

Kim, D., & Ammeter, T. (2014). Predicting personal information system adoption using an integrated diffusion model. *Information and Management*. https://doi.org/10.1016/j.im.2014.02.011

Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2012*, *March*, 340–345. https://doi.org/10.1109/PerComW.2012.6197507

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery*, *88*(March). https://doi.org/10.1016/j.ijsu.2021.105906

Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., & Koffel, J. B. (2021). PRISMA-S: an extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews. *Systematic Reviews*, *10*(1), 39. https://doi.org/10.1186/s13643-020-01542-z

Salleh, N., Hussein, R., Mohamed, N., & Aditiawarman, U. (2013). An empirical study of the factors influencing information disclosure behaviour in social networking sites. *Proceedings - 2013 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013*, 181–185. https://doi.org/10.1109/ACSAT.2013.43

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, *22*(5), 428–438. https://doi.org/10.1016/J.INTCOM.2010.05.001

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

Zhang, K. Z. K., & Benyoucef, M. (2016). Consumer behavior in social commerce: A literature review. *Decision Support Systems*, *86*, 95–108. https://doi.org/10.1016/J.DSS.2016.04.001

Zhu, P., Hu, J., & Zhu, X. (2020). Research on the Influence of Fear Appeal on APP Users' Privacy Protection Behavior: An Empirical Study. *IOP Conference Series: Materials Science and Engineering*, *782*(4). https://doi.org/10.1088/1757-899X/782/4/042011.