Cihan University-Erbil Scientific Journal (CUESJ)

Review Article

Social Network Privacy Models: A Systematic Literature Review and Directions for Further Research

Abdullah Abdulabbas Nahi Al-Rabeeah[1*], Mohammed Mahdi Hashim[2]

[1]Department of Computer Science, Cihan University-Erbil, Iraq, [2]Department of Computer Science, Auruk University, Baghdad, Iraq

ABSTRACT

Privacy is a vital research field for social network (SN) sites (SNS), such as Facebook, Twitter, and Google+, where both the number of users and the number of SN applications are sharply growing. Recently, there has been an exponential increase in user-generated text content, mainly in terms of posts, tweets, reviews, and messages on SN. This increase in textual information introduces many problems related to privacy. Privacy is susceptible to personal behavior due to the shared online data structure of SNS. Therefore, this study will conduct a systematic literature review to identify and discuss the main privacy issues associated with SN, existing privacy models and the limitations and gaps in current research into SN privacy.

Keywords: Component, privacy models, privacy rules, social network, social network privacy

INTRODUCTION

Social network (SN) has currently become a significant platform for users to share newscasts, thoughts, and post messages. As pointed out by Gritzalis et al.,[1] the introduction of Web 2.0 contributed to the growing number of users using SN sites (SNS). Users can now interact with each other, generate, or reorganize information and thoughts, and express themselves in computer-generated communities. Such means of communication, along with the mutuality of user-generated content, are referred to as SNS. Millions of people are using SNS such as Google+, Facebook, Twitter, and Instagram for daily activities. There is more than one type of SNS with numerous affordances in the technological aspects, interests. Moreover, their key technological features are coordinated, and the cultures that arise around SNS are assorted. Most sites help strangers to connect, based on shared interests, political opinions, or activities. Some sites are provided to varied users, while other sites are targeted toward interested people, based on common language, or shared cultural, sexual or religious interests, or nationality-based. Sites also vary in the extent to which they incorporate new information and communication tools, such as mobile connectivity, blogging, and photo/video-sharing. In recent years, there has been an exponential increase in user-generated text content, mainly in terms of posts, tweets, reviews, and messages on SN. This increase in textual information introduces many problems related to privacy. Thus, due to the need for user privacy protection in SN, many privacy tools are employed.[2] This paper conducts a systematic literature review on the privacy of SNS since there are many problems not solved yet related to privacy.

SN

SN is a site or system of associations and connections.[3] In addition, it has another definition. These include Facebook, LinkedIn, Twitter, or content sharing systems, for example, YouTube and Flickr. In these (and other) SNS, the user tries to find similar or perfectly matched individuals with similar interests or encounters. SN includes components of different sorts of data, for example, music, photographs, recordings, websites, connections, and outsider applications. Table 1 illustrates the SN definitions from earlier researchers.

The well-known SN with their main focus, default relationships, and the direction of the relationships is shown in Table 2.

Review Method

This study uses a systematic review approach to answer the questions posed above. (Alvarez-Jimenez and Alcazar-Corcoles

Corresponding Author:
Abdullah Abdulabbas Nahi Al-Rabeeah, Department of Computer Science, Cihan University-Erbil, Iraq.
E-mail: abdullah.nahi92@gmail.com

Received: Apr 18, 2019
Accepted: Apr 25, 2019
Published: Aug 20, 2019

DOI: 10.24086/cuesj.v3n2y2019.pp92-101

Table 1: SN definitions from earlier researchers

No.	Definitions	Reference
1.	The usage of SN by an organization in communication with outside parties such as clients, sellers, and the community	Leonardi *et al*. 2013[4]
2.	SNS are web-based services that allow individuals to[1] construct a public or semi-public profile within a restricted system,[2] create a list of additional users with whom they share a link, and[5] view and traverse their list of connections and those made by others within the system. The nature and terminology of these connections may vary from site to site	Ellison and Boyd 2007[3]
3.	User profiles that describe their locations, interests, and education background, and provide useful information differing from links	Croitoru *et al*., 2013[6]
4.	SNs provide users, within their platforms, with powerful ways to interact with other users through different forms and modalities. Consequently, each user can search and check the profiles of other SN members (for various reasons), exchange messages with some of them, publish videos, and post comments on shared photos, etc.	Hajli 2013[7]
5.	SNS are for finding old friends, meeting new friends, or finding people who have the same interests or problems across political, economic, and geographic borders. By creating personal information profiles that contain information such as photos, video and audio files, SNS allow users to connect, post messages, send e-mails, and instant messages to each other	Abawajy *et al*., 2016[8]
6.	The infrastructure of SNs can support a rich variety of data analytics applications such as search, text analysis, image analysis, and sensor applications	Aggarwal and Wang 2011[9]
7.	SN technologies have opened new possibilities for sharing personal information with online networks, and millions of people routinely self-disclose personal information on SNSs	Bazarova and Choi 2014[10]

SNS: Social network sites, SN: Social network

2014) An effective review can create a firm foundation for advancing knowledge, facilitate theory development and discover areas where the research is needed.[12] A systematic review can be defined as a process of identifying, evaluating, and interpreting all available research relevant to research questions, area of study, or a rising phenomenon of interest.[13] The reasons for conducting a systematic review are to summarize the evidence about technology or treatment, summarize the evidence of the advantages of a specific method, identify any research gaps in the existing research and provide deep understanding for new phenomena.[13] Therefore, these reasons fit with the aim of our review. This study follows Kitchenham and Charters guidelines, where a systematic review task involves three main stages: Planning the review, conducting the review, and reporting the review. Each stage has certain activities.

Review protocol

Review protocol is an essential stage in performing a systematic review and specifies the methods that will be used to undertake a systematic review. Figure 1 shows the review protocol stages. The goal of a review protocol is to reduce research bias.[13] The review protocol includes background, research questions, search strategy, study selection process, data extraction, and synthesis of the extracted data.[13] In this review, the research questions and background of SN are stated above. Figure 1 illustrates the review protocol used for this study.

INCLUSION AND EXCLUSION CRITERIA

The purpose of identifying inclusion and exclusion criteria is to make sure that the selected studies are relevant and related to our study. Because this review focuses on understanding the SN, the consideration is only on articles from journals, conferences, workshops, book chapters, and symposia in the English language. The duration of the period of publication of the selected studies is from 2006 to 2017. The reasons for choosing this period are two-fold. First, this review is complementary to previous efforts[14] to provide a deep understanding of SN. Second, the term SN has been increasingly used in various studies since 2008, and the previous major articles reviewing the state of SN research cover literature until this year, therefore, this year is required to systematically collect, analyze, and synthesize these studies for past 6 years. Table 3 shows the criteria for this review.

Table 2: Well-known SN with their main focus, default relationship, and the relationships direction (Gitelman 2006)[11]

SN platform	Focus	Default relationship (S)	Relationship direction
Facebook	General use	Friendship	Symmetrical
Flicker	Photo sharing	Contact and optionally friend, or family	Symmetrical
Google+	General use	Friends, family, acquaintances	Symmetrical
LinkedIn	Professional	Business	Symmetrical
Twitter	Microblogging	Followers	Asymmetrical
YouTube	Video sharing	Subscribe-to	Asymmetrical

SN: Social network

Search Strategy

The search strategy, as depicted in Figure 1, consisted of two stages: An automatic stage and manual stage. The automatic stage was to identify the primary studies of SN. Based on Webster and Watson's recommendations,[12] the researchers did not limit the search process to a specific set of journals; instead, and several online databases were used to cover a broad range of academic publications. The online databases used were ScienceDirect, Scopus, Springer, IEEE Explorer, and Web of science. These databases are considered relevant and provide high impact factor publications. To perform the automatic

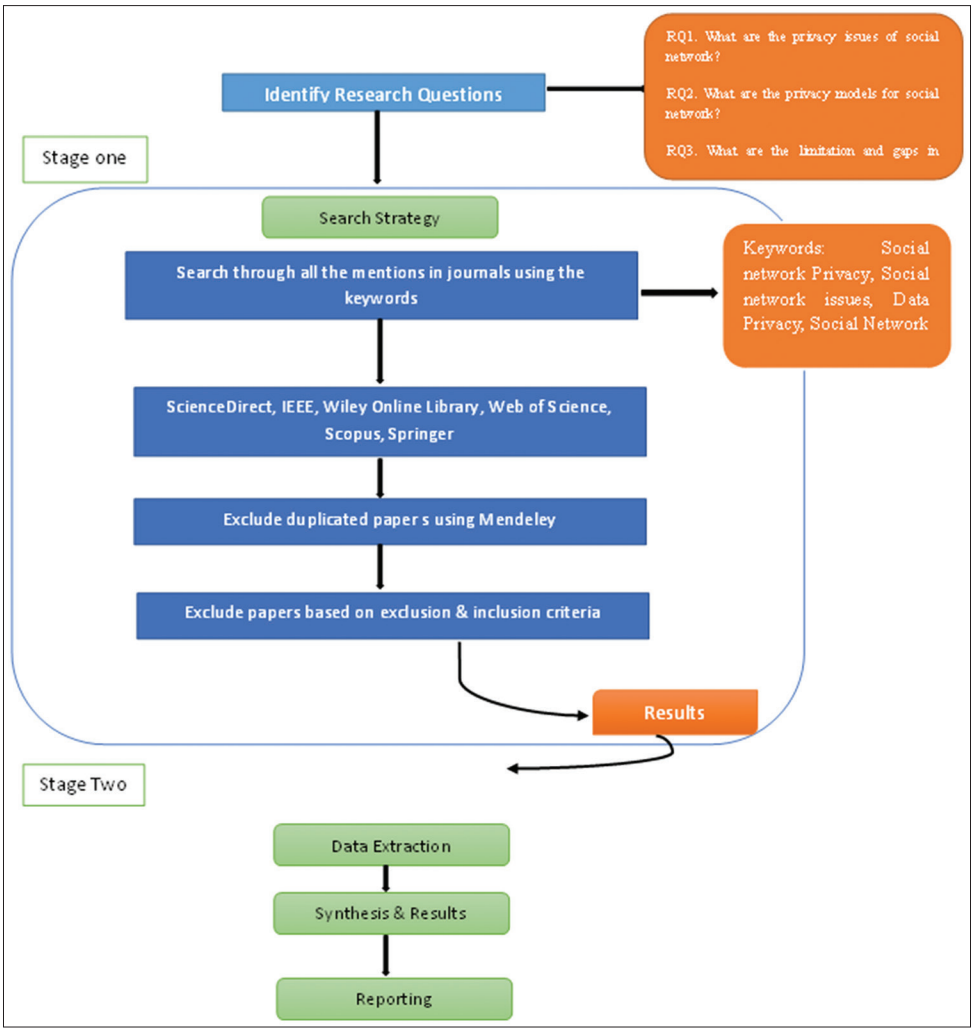

Figure 1: Research methodology

Table 3: Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Full-text	Uncompleted studies
Published within the selected period (2006–2017)	Non-English
Published in the above-selected database written in English	Outside the selected time study manuscript
In the domain of social network	Duplicated studies

search, keywords were identified based on the research question of this review. The main keywords used were: "SN," "SN privacy," and "SN privacy issues." The second stage was a manual search. Backward and forward search methods[12,15] were used to trace the citation of the selected studies. We used the Google Scholar search engine to go forward and find the studies which were cited in the selected primary studies. The manual stage was used to ensure that the systematic search was comprehensive and relatively complete.[12] For managing and sorting all the studies, Mendeley, a reference management tool, was used to keep all the search results and easily remove the duplicated studies.

Study selection process

The study selection process was used to identify the studies related to the research questions of this review. Using the defined keywords, the result of the initial search identified 185 studies from the automatic search. After removing the duplicated studies using Mendeley, 150 remained. We then applied the inclusion/exclusion criteria, on the abstract and conclusion of each study. In this step, 90 studies were eliminated. Based on Kitchenham and Charters' recommendation,[13] we excluded the studies that were clearly not related to the subject of this review. Full-text scanning was used for the remaining studies, with the consideration of the exclusion criteria. We also applied the manual search to the reference list of each study, to trace any missing studies. After applying the manual search, an additional 12 studies were found. Thus, the final set of primary studies was 72. Finally, we applied quality assessment criteria, and 12 were removed; thus, a total of 60 studies were identified as a final list of primary studies. Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

Quality assessment

Applying quality assessment is considered critical to assessing the quality of the primary studies.[13] The details of quality assessment are based on quality instruments, which could be a checklist of factors or questions that need to be applied for each study.[16,17] In this review, we developed the following three quality assessment criteria to assess the quality of each study:

QA1. Is the topic addressed in the paper related to SN privacy?
QA2. Is the research problem described clearly in the paper?
QA3. Is the data collection method described in the paper?

The three QA criteria presented above were applied to the 72 primary studies to increase our confidence in the credibility of the selected studies. The process of applying quality assessment used three levels of the quality schema (high, medium, and low),[18] in which the quality of each study depends on the loading score. For instance, studies that fulfill the criterion will be given 2; studies that partially fulfill the criterion will be given 1; and studies that do not fulfill the criterion will be given.

Studies that score 5 or above will be considered high quality, while if they score 4 they will be considered medium, while if they are below 4 they are considered low. After applying the QA, 12 studies were eliminated because they did not fulfill the QA criteria. The results of the QA are displayed in Figure 2.

Research questions results

RQ1. What are the privacy issues in SN?

The two concepts of privacy concerns and privacy attitudes are basically different. Privacy concerns could be quite generic and in most cases are not bound to any specific context, while privacy attitudes refer to the assessment of exact privacy behaviors.[19] Another stream of study aimed to understand self-disclosing behavior in online SN (OSN), especially among young people. Barnes[20] uses the term privacy paradox about the privacy behavior of young people in SN. Young people tend not to realize that SM provides public space and disclose personal information that could perhaps be misused.[20]

Carrascal et al.,[21] led an experiment aiming to determine the monetary value of several kinds of personal information.

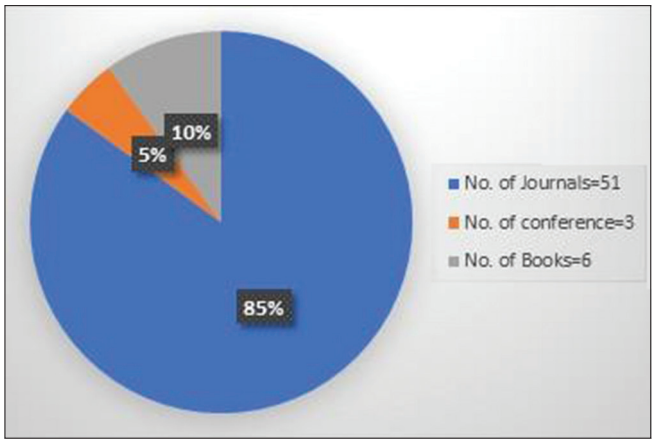

Figure 2: Review protocol

Using a web browser plugin, they prompted users to value their personal data at the time and place they were produced. In the first phase of the experiment, the browser plugin collected data about the browsing behavior of each subject. Data were used to calibrate the behavior of the plugin in the second phase. In the second stage, the plugin exhibited popups as the participants were browsing the internet. Popups contained two kinds of questions: Questions about evaluating personal information and questions on participants' privacy perceptions and knowledge. Information valuation questions were framed as auctions.[21] For instance, one question was, "What is the questionnaire on privacy attitudes and preferences and, then, to visit an online store." During their shopping in the store, they were engaged in a sales dialogue with an anthropomorphic three-dimensional shopping bot. Participants answered most of the questions, even if these were highly personal. This indicates that even though internet users claim that privacy is a high priority, they do not behave accordingly. Based on a questionnaire survey and an examination of participants' Facebook profiles, Hughes-Roberts 2013) 23 concluded that a general statement of user concern is not a valid indicator of privacy behavior within the network. However, he questioned the appropriateness of surveys as instruments for studying the privacy paradox.[22] Lee[23] confirmed the existence of an attitude versus behavior dichotomy. They conducted a series of semi-structured in-depth interviews and an experiment to assess the influence of expected benefit and expected risk on users' intention to share personal information. They concluded that users actively share personal information despite their concerns because they do not only consider risk but also the expected benefit of sharing.[24] Reynolds et al., in their study, also found that there was little correlation between participants' broader concern about privacy on Facebook and their posting behavior.[25] In contrast to Tufekci,[26] they found that the portion of posts that were visible to a large audience appeared to be independent of general privacy attitude. A web survey by Taddicken also showed that privacy concerns hardly impact self-disclosure.[27] The relationship between privacy concerns and self-disclosure is moderated by various variables. Perceived social relevance and the number of other social web applications used have a strong moderating effect. In this study, social relevance mainly refers to the disclosing behavior of communication partners indicating that disclosure proceeds on a quid pro quo basis, i.e., "you tell me and I tell you." A study by Zafeiropoulou et al.,[28] specifically examined location data, which are a form of personal information increasingly used by mobile applications. Their survey also found evidence that supports the existence of the privacy paradox for location data. In their book Liquid Surveillance, Bauman and Lyon talk about privacy in relation to online web-based social networking administrations. Bauman says: "We present our rights to privacy for butcher of our own will. Or, then again maybe we simply agree to the loss of privacy as a sensible cost for the marvels offered in return". Or, then again, the weight to convey our own self-sufficiency to the slaughterhouse is so overpowering, so near the state of the rush of sheep, that exclusive of a couple especially defiant, striking, contentious and unfaltering wills are set up to make a sincere endeavor to withstand it.[29] This is an instance of the unavoidable negativity show in discourse about insurance and an instance of privacy being discussed as a generalizable thing with a lone definition

material to everyone. It has presented the usage of online electronic long range informal communication organizations as the opposite of assurance. Bauman and Lyon proceed to express their view that there has been an alteration in people's points of view about what ought to be open and what ought to be private.[29] The authors believe that this change has been made by the coming of widespread use of online web-based SN administrations. Both methodologies comprehensively characterize the philosophical utility of privacy. Legal privacy, for instance, doubts about the ancient rarities of privacy, for example, the data, while social privacy is concerned with the impacts of association of people in the public eye on privacy. While there might be examples in which the two may cross, making a distinction between the two toward the start of this review is essential as it shows the wide remit of the review. Even scholars with a legal background have highlighted the social aspects of privacy.[30] Valerie[29] puts forward comparable assumptions, highlighting that privacy can be normally comprehended in the everyday transactions of social standards inside connections. This show how social privacy as an idea is fundamentally concerned with how people communicate with each other. In any case, given the unfathomable sorts of communications that take place between people, social privacy soon turns out to be a very wide concept. Diverse ways to deal with understanding social privacy have been looked for organizations such as Facebook and Twitter. They also conducted a survey that revealed a strong correlation between information privacy concern and all types of responses, except for misrepresentation. Contrary to previous research, Blank et al.,[32] found that younger people are more likely to take action to protect their privacy than older ones. In addition, studies show a positive correlation between privacy concerns and protection behavior. Lutz and Strathoff[33] conducted a telephone survey in Switzerland employing a questionnaire that covered several privacy-related constructs. This survey confirmed a weak but statistically significant influence of privacy concerns on protection behavior. Recent surveys show that privacy concerns trigger protective responses, such as uninstalling mobile applications. A survey of smartphone users by the Pew Internet Project[34] revealed that 54% of the mobile application users surveyed had decided to not install a cell phone application when they discovered how much personal information they would need to share to use it and 30% of the cell phone application users had uninstalled an application that was already on their cell phone because they learned it was collecting personal information that they did not wish to share. On the other hand, only 19% of cell phone owners had turned off the location tracking feature on their cell phone. Table 4 shows that the studies reviewed and the methodology they used for collecting the data and how such as.[26,35-38]

RQ2. What are the privacy models in SN?

Several studies have built different models explaining mechanisms of user privacy on the internet. Many of them cover issues arising when users make decisions about exposing their private information in exchange for service use, such as online shopping, internet banking, or the use of the internet in general. A limited number of studies also address issues of privacy when users communicate with other users in addition to the service users in the context of OSN. Nov and Wattal[39] investigated privacy issues of SN. In this study, they extended earlier research on web privacy to address inquiries regarding precursors of privacy concern in social groups, and in addition, the effect of privacy concern in such groups. In the group and the group's data sharing standards negatively affected the group members' particular privacy concerns. They likewise found that group-specific privacy concerns not only led members to embrace more prohibitive data sharing settings but also additionally diminished the amount of data they imparted to the group. Additionally, found find that data sharing was affected by system centrality. In another exploration, Chai et al.[40] analyzed variables that impact web clients' private data sharing conduct among groups of preteens and early high schoolers, which are among the most powerless gatherings on the web. This review study provides an examination system that clarifies a web client's data conduct in ensuring privacy. Two noteworthy components were found to influence web clients' data privacy practices: (1) Clients' apparent significance attached to data privacy and (2) data privacy self-adequacy. The review, additionally, found that clients have confidence in the estimation of online data privacy and that data privacy assurance conduct differs according to gender. Shin[41] analyzed privacy, trust, and privacy concern in the context of interpersonal interaction websites among purchasers, utilizing both solid scales and measures. She proposes a SMS acknowledgment show

Table 4: Studies on social network privacy

Study	Context	Methodology	Participants
Bamas (2011)[35]	SNSs	Student Survey	Students
Carrascal (2013)[21]	SNSs	Survey	Web users
Hughes-Roberts (2013)[23]	SNSs	Survey	Students
Hau *et al*. (2013)[24]	SNSs/Location Data	Experiments	Users of SNSs
Reynolds *et al*. (2011)[25]	SNSs	Survey	Facebook
Tufekci (2008)[26]	SNSs	Survey	Students
Taylor *et al*. (2013)[36]	SNSs	Survey	Students
Blank *et al*. (2014)[32]	SNSs	Survey	Random users
Boyd *et al*. (2010)[37]	SNSs	Survey	Students
Christofides *et al*. (2009)[38]	SNSs	Survey	Students
Lutz and Strathoff (2014)[33]	Internet use/SNSs	Survey	Sample users

by coordinating intellectual and in addition full of feeling mentalities as essential affecting components, which are driven by fundamental convictions, visual privacy, visual privacy, trust, disposition, and aim. This is the outcome of a study of SMS clients which confirmed that the proposed hypothetical model clarifies and predicts client acceptance of SMS significantly well. The model shows phenomenal estimation properties and builds up visual privacy, and visual privacy of SMS as particular develops. The finding additionally uncovered that apparent privacy affects the impact of visual privacy on trust. Nov and Wattal[39] investigate privacy issues of social processing condition. In this study, they stretch out earlier research on web privacy to address inquiries regarding precursors of privacy concern in social registering groups, and in addition, the effect of privacy concern in such groups. The outcomes demonstrate that clients' trust in other group individuals and the group's data sharing standards negatively affect group privacy concerns. They likewise distinguish that group privacy concerns not just lead clients to embrace more prohibitive data sharing settings, additionally diminish the measure of data they impart to the group. In addition, they find that data sharing is affected by system centrality and the residency of the client in the group.

Shin[41] examined security, trust, and privacy concerns with regard to social networking websites among consumers using reliable scales and measures. The study proposes an SNS acceptance model by integrating cognitive as well as affective attitudes as primary influencing factors, which are driven by underlying beliefs, perceived security, perceived privacy, trust, attitude, and intention. Results from a survey of SNS users validated that the proposed theoretical model explains and predicts user acceptance of SNS substantially well. The model shows excellent measurement properties and establishes perceived privacy and perceived the security of SNS as distinct constructs. The finding also reveals that perceived security moderates the effect of perceived privacy on trust.

In contrast to theory-based approaches, bottom-up approaches of model construction and testing make their contribution to theory building from a selected pool of salient constructs, such as trust,[42,43] weakness,[44] or individual demeanor.[45,46]

Malhotra et al.[46] focus on three distinct yet closely related issues. First, drawing on social contract theory, the authors offered a theoretical framework on the dimensionality of Internet Users' Information Privacy Concerns (IUIPC). The authors then attempted to operationalize the multidimensional notion of IUIPC using a second-order construct and develop a scale for it. Finally, they proposed and tested a causal model on the relationship between IUIPC and behavioral intention toward releasing personal information at the request of a marketer. The results of this study indicate that the second-order IUIPC factor, which consists of three first-order dimensions, namely, collection, control, and awareness, exhibited desirable to user's psychometric properties in the context of online privacy. In addition, their causal model centering on IUIPC fits the data satisfactorily and explains a significant amount of variance in behavioral intention, suggesting that the proposed model will serve as a useful tool for analyzing online consumers' reactions to various privacy threats on the Internet Dinev and Hart[44] developed and validated an instrument to measure the privacy concerns of individuals who use the internet and two antecedents, perceived vulnerability and perceived ability to control information. The results of an exploratory factor analyses supported the validity of the measures developed. In addition, the regression analysis results of a model including the three constructs provide strong support for the relationship between perceived vulnerability and privacy concerns, but only moderate support for the relationship between perceived ability to control information and privacy concerns. The authors claim that the relationship among the hypothesized and privacy concerns may be one that is more complex than is captured in the hypothesized model, considering the strong theoretical justification for the role of information control in the extant literature on information privacy.

In the realm of OSNs, several studies have challenged the common assumption that young people do not protect their private information contrary to previous research, Lutz and Strathoff[33] found that younger people are more likely to act to protect their privacy than older ones. Young people use a variety of protection strategies, such as using pseudonyms and giving false information,[47] restricting access to their profiles and adjusting their privacy settings,[48] limiting friendship requests, and deleting tags and photos.[49] In addition, studies show a positive correlation between privacy concerns and protection behavior Aeschlimann et al.[50] conducted a telephone survey in Switzerland employing a questionnaire that covered several privacy-related constructs. This survey confirmed a weak but statistically significant influence of privacy concerns on protection behavior.

Casalo et al.[51] investigated the impact of perceived site privacy, ease of use, and notoriety on buyer confidence with regards to web-based keeping money. The study also breaks down the trust-duty relationship, since responsibility is a key variable for building up effective long-term associations with clients. Their study presents the result of privacy ease of use and reputation on buyer confidence in a site in the web-based managing an account setting. In addition, it proposes that trust positively affects purchaser responsibility, convenience and reputation have an immediate and huge impact on shopper confidence in a money-related administration site. In addition, purchaser trust is strongly identified with relationship. In addition, it is noted that trust is a key moderating element in the improvement of relationship responsibility in the web-based saving money setting. Hence,[52] build-up a hypothetical system portraying the trust-based basic leadership prepares a purchaser uses when making a purchase from a given webpage, and test the proposed display utilizing a structural equation modeling strategy on web buyer purchasing behavior, with information gathered by means of a web survey. The results of the survey indicated that web buyers' trust and perceived risk affect their purchasing choices. Customer intention to trust, reputation, privacy concerns, privacy concerns, the data nature of the website, and the organization's reputation effectively affect internet buyers' trust in the website. Bandyopadhyay et al.[53] proposed a hypothetical system to explore the elements that impact the privacy concerns of customers who utilize the internet and the results of such privacy concerns. Elements

distinguished as precursors to online privacy concerns are seen as a weakness to accumulation and abuse of individual information, perceived capacity to control information gathering and its resulting utilization, the individual's level of internet proficiency, social awareness, and underlying social variables. The possible outcomes of online privacy concerns are the unwillingness to give individual data on the web, shunning web-based businesses, or even unwillingness to utilize the internet. The model explored depends on a correspondence theory (i.e., Communication Privacy Management [CPM] theories).

A genealogical or family tree is the main component to build their trust model. There exist many sites to manage a family tree. However, those are not popular as SNS. On the other hand, many popular SNSs are not focused on creating a family tree. Although the notion of the family tree is absent in these sites, often family members coexist in the same network as a friend or follower or fan. Hence, they can easily build a family tree even if it does not exist in the architecture of the SMS. Using the family tree, they propose their novel approach for securing SN by calculating trust. To realize trust quantitatively, they compute two quantities for the trust baseline:

a. Trust value and (b) trust score: Trust value captures the static component of human trust while trust score changes dynamically with human connection in SMS. Both of those trust indicators are based on generation circle.[54] SN users dissatisfied with the SNSs request for SN login credentials may also engage in public action as a form of recourse or to seek a remedy. Perales et al.[55] identify two such public actions: Complain to the company and complain indirectly to a third party. Given the nature of interviews, individuals are not likely to complain about the requesting during them. Instead, they focus on complaints to companies' executives. Indirectly complaining to a third party may include contacting the media or local politicians to seek redress. Ngai et al.[56] point out that SN applications are multi-disciplinary, including such areas as marketing, knowledge sharing, customer relationship management, collaborative activities, organizational communications, education, and training. The design and development of each application system are underpinned by different personal and social behavior theories and models, including personal behavior theories (e.g., personal traits, TAM, TRA, and Theory of Planned Behavior [TPB]), social behavior theories (e.g., social capital, social cognitive, and social power), and mass communication theories (e.g., PSI and uses and gratifications theory), and are encompassed by a wide variety of SN tools and technologies, such as media sharing sites (e.g., YouTube and Instagram), blogs and microblogs (e.g., Twitter and Weibo), social bookmarking sites (e.g., Delicious and Pinterest), virtual and online communities (e.g., Lonely Planet and Yahoo Answers), SMS (e.g., Facebook and LinkedIn), and virtual worlds (e.g., Second Life and Active World). Using this model, they argue that when researchers and system developers design and develop SN applications, they should first understand the theoretical foundations of a system, and based on these foundations, choose the right tools and technologies, and process the design, development, and implementation of the system. Private action by Kim and Ko,[52] information privacy can be undermined when internet clients lose control over how online organizations gather and handle their own data.[46] Cases of such loss of control range from getting undesirable emails. The term Social Computing according to Nov and Wattal[39] alludes to applications and administrations that encourage aggregate activity and social cooperation on the web, for example, sites, wikis, interpersonal organizations, and dialog discussions. As social computing is turning into an essential part of people's groups' and social status, it has been receiving increasing research interest. The achievement of social networking frameworks, whose content is made altogether by client commitment, relies on the ability of the members to share. As indicated by the privacy analytics theories, people's readiness to provide data is, thus, represented by their privacy concerns. To address this. This issue is by all accounts, especially imperative given that interpersonal organizations, for example, Facebook have been confronting increasing criticism over their privacy arrangements.

Chai et al.[57] propose a connection between apparent significance of data privacy to web users and their conduct in ensuring their privacy on the web. As observed in past research a positive connection was demonstrated between perceived significance in a specific area and behavioral intention to carry out the activities identified with that area, they expect that web clients who put a higher importance on the significance of data privacy will exhibit an even stronger propensity to show online privacy assurance behavior than the users who place lower importance on the significance of data privacy on the web. All the factors that will affect the user privacy such as sex, Age, Education, etc.[58] As they point out, the IUIPC will play a main role in the future.

CPM theory asserts that people control their private information based on the use of personal privacy rules. Through developing, learning, and negotiating rules depending on culture, gender, motivation, context, and risk/benefit ratio, people coordinate boundary linkages, boundary permeability, and boundary ownership. The theory delineates such causal relationships in a qualitative and interpretive manner, while the TPB outs forward a mechanism for the human decision-making process, i.e., a causal link constituting a person's salient beliefs and evaluations, attitude toward a behavior, and behavioral intentions. Table 5 illustrates the theories and research constructs for the SN privacy.

RQ3. What are the limitation and gaps in current research regarding SN privacy?

Privacy concerns exist about the potential for the collection, retention, and data mining of personal information by the federal government of the USA with respect to its use of SN for disaster recovery purposes. Specifically, the use of status alerts and the creation of personal pages to establish situational awareness may raise privacy concerns.[61] Others are concerned about how the information might be used, for example, would the federal government compile records after a terrorist attack to help investigate certain individuals or some concerned about the user behavior itself in the SN

Table 5: Theories and research constructs for SN privacy

Study	Base theories	Research constructs
Lallmahamood, 2007[58]	Technology acceptance model	Perceived privacy perceived usefulness/perceived ease of use, Intention to use internet banking
Wang *et al*., 2012[59]	Reasoned action	(Subjective norm/attitudes toward internet shopping), intention to shop on internet
Kim and Ko 2011[52]	Reasoned action	IP concern/perceived justice/social benefits from complaining/information privacy-protective responses
Jordan 2015[54]	Trust theory	Privacy, personal behavior, family attitude
Posey 2016[60]	Extended ethical decision-making model	Information privacy protection
Eric *et al*., 2015[58]	Personal behavior	SN privacy
Lee 2013[23]	CPM/TPB	SN privacy

SN: Social network, CPM: Communication Privacy Management, TPB: Theory of Planned Behavior

by going through all the previous studies shows the user's attitude can be affected by many factors that will cause itself privacy.[23] A lot of research focused on the users' behavior but did not consider all the factors that may affect the user privacy, depending on many important reasons, more importantly, the huge development happening in SN platforms and the number of users that are reaching billions of daily users using at least one SN platform.[62] Smith *et al*.[63] point out that privacy for users is almost not available in the data or information has been posted into SNs. The modern smartphones have made the using of SN very easy and accessible everywhere since the proliferation of high-speed mobile networks is enabling a culture of impulsive and carefree posting of user content. For instance, according to Facebook statistics, the scale of this phenomenon per month has risen from two billion to over six billion and there were one billion active users on average at the end of 2016 on a daily basis.[64] Almost most of the photos posted on SN have no relevance to privacy as from a personal perspective. From previous studies, the current models do not seem to cover all the required needs for SN users and according to Marwick and Boyd[65] the privacy challenges increasing day by day since the development of SNS growing very fast and the number of users is around one billion for each platform. Several studies have built causal models explaining mechanisms of user privacy on the internet. Many of them cover issues when users make decisions of exposing their private information in exchange for service use, such as online shopping, internet banking, or the use of internet in general. However, a limited number of studies have addressed issues of privacy when users communicate with other users in addition to the service use in the context of OSN.

CONCLUSION AND RECOMMENDATION

This study provides an overview of the privacy concept in SN. To understand SN privacy, we set three research questions related to the nature of SN privacy. A systematic review approach was used to answer these questions; the review included the studies published between 2006 and 2017. After performing multiple selection processes, 60 studies were selected that focus on SN privacy. The remainder of the studies was eliminated from the review as they did not fulfill the inclusion criteria or have not reached the quality level. The study provides a clear view of SN privacy and privacy models by identifying the privacy in SN, and the main issues could be affecting the user privacy. From the data analysis, the majority of the 60 studies belong to user behavior and platforms privacy rules themes, while other areas received little attention, such as government law, business model, and security and privacy issues. In addition, the research methodologies used in these studies were identified and classified. The study found that more studies focused on the privacy of the users in SNS by depending on different factors that were used previously, because of the huge number of the users in the SNS.

REFERENCES

1. D. Gritzalis, M. Kandias, V. Stavrou and L. Mitrou. "History of information: The case of privacy and security in social media". Proceeding of the History of Information Conference. pp. 283-310, 2014.
2. H. Zhu, C. Huang, R. Lu and H. Li. "Modelling information dissemination under privacy concerns in social media". *Physica A: Statistical Mechanics and its Applications,* vol. 449, pp. 53-63, 2016.
3. N. B. Ellison and D. M. Boyd. "Social network sites: Definition, history, and scholarship". Journal of Computer-Mediated Communication, vol. 13, pp. 210-230, 2007.
4. P. M. Leonardi, M. Huysman and C. Steinfield. "Enterprise social media: Definition, history, and prospects for the study of social technologies in organizations". *Journal of Computer-Mediated Communication*, vol. 19, pp. 1-19, 2013.
5. T. K. Yu and G. S. Wu. "Determinants of internet shopping behavior: An application of reasoned behaviour theory". *International Journal of Management*, vol. 24, p. 744, 2007.
6. A. Croitoru., A. Crooks, J. Radzikowski and A. Stefanidis. "Geosocial gauge: A system prototype for knowledge discovery from social media". International Journal of Geographical Information Science, vol. 27, pp. 2483-2508, 2013.
7. M. Hajli. "A research framework for social commerce adoption". *Information Management and Computer Security*, vol. 21, pp. 144-154, 2013.
8. J. H. Abawajy, M. I. H. Ninggal and T. Herawan. "Privacy preserving social network data publication". *IEEE communications Surveys and Tutorials*, vol. 18, pp. 1974-1997, 2016.
9. C. C. Aggarwal and H. Wang, H. "Text mining in Social Networks". In: *Social Network Data Analytics*. Springer, Berlin, Germany. pp. 353-378, 2011.
10. N. N. Bazarova and Y. H. Choi. "Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites". *Journal of Communication*,

vol. 64, pp. 635-657, 2014.
11. L. Gitelman. "Always already new". In: *Media, History, and the Data of Culture*. The MIT Press, Cambridge. P. 7, 2006.
12. J. Webster and R. T. Watson. "Analyzing the past to prepare for the future: Writing a literature review". *MIS Quarterly*, vol. 26, no. 2, pp. 13-23, 2002.
13. P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner and M. Khalil. "Lessons from applying the systematic literature review process within the software engineering domain". *Journal of Systems and Software*, vol. 80, pp. 571-583, 2007.
14. M. Shanmugam and Y. Y. Jusoh. "Social Commerce from the Information Systems Perspective: A Systematic Literature Review". Computer and Information Sciences (ICCOINS), 2014 International Conference. IEEE. pp. 1-6, 2014.
15. Y. Levy and T. J. Ellis. "A systems approach to conduct an effective literature review in support of information systems research". *Informing Science: The International Journal of an Emerging Transdiscipline*, vol. 9, pp. 181-212, 2006.
16. W. Bandara, S. Miskon and E. Fielt. "A Systematic, Tool-supported Method for Conducting Literature Reviews in Information Systems". Proceedings of the19th European Conference on Information Systems (ECIS 2011), 2011.
17. B. Kitchenham, D. Budgen, P. Brereton, M. Turner, S. Charters and S. Linkman. "Large-scale software engineering questions expert opinion or empirical evidence"? *IET Software*, vol. 1, pp. 161-171, 2007.
18. S. Nidhra, M. Yanamadala, W. Afzal and R. Torkar. "Knowledge transfer challenges and mitigation strategies in global software development a systematic literature review and industrial validation". *International Journal of Information Management*, vol. 33, pp. 333-355, 2013.
19. S. Kokolakis. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". *Computers and Security,* vol. 64, pp. 122-134, 2017.
20. S. B. Barnes. "A privacy paradox: Social networking in the United States". *First Monday*, vol. 11, pp. 15, 2006.
21. J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini and R. de Oliveira. "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online". Proceedings of the 22nd International Conference on World Wide Web. ACM. pp. 189-200, 2013.
22. T. Hughes-Roberts. "Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour"? Social Computing (SocialCom), 2013 International Conference. IEEE. pp. 909-912, 2013.
23. K. J. Lee. "Development and Analyses of Privacy Management Models in Online Social Networks based on Communication Privacy Management Theory". PhD Thesis, Drexel University, 2013.
24. Y. S. Hau, B. Kim, H. Lee, Y. G. Kim. "The effects of individual motivations and social capital on employees' tacit and explicit knowledge sharing intentions". *International Journal of Information Management*, vol. 33, pp. 356-366, 2013.
25. B. Reynolds, J. Venkatanathan, J. Gonçalves and V. Kostakos. "Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours". IFIP Conference on Human-Computer Interaction. Springer, Berlin, pp. 204-215, 2011.
26. Z. Tufekci. "Can you see me now? Audience and disclosure regulation in online social network sites". *Bulletin of Science, Technology and Society,* vol. 28, pp. 20-36, 2008.
27. M. Taddicken. "The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure". *Journal of Computer-Mediated Communication*, vol. 19, pp. 248-273, 2014.
28. A. M. Zafeiropoulou, D. E. Millard, C. Webber and K. O'Hara. "Unpicking the Privacy Paradox: Can Structuration Theory Help to Explain Location-Based Privacy Decisions"? Proceedings of the 5th Annual ACM Web Science Conference. ACM, pp. 463-472, 2013.
29. Z. Bauman and D. Lyon. "Liquid Surveillance: A Conversation". John Wiley and Sons, New York, 2013.
30. J. Grimmelmann. "The privacy virus". *Facebook and Philosophy*, vol. 6, pp. 3-12, 2010.
31. D. C. Locke and D. F. Bailey. "*Increasing Multicultural Understanding*". Sage Publications, Thousand Oaks, 2013.
32. G. Blank, G. Bolsover and E. Dubois. "A New Privacy Paradox: Young People and Privacy on Social Network Sites". Prepared for the Annual Meeting of the American Sociological Association, 17 August 2014. San Francisco, California, 2014.
33. C. Lutz and P. Strathoff. "Privacy Concerns and Online Behavior Not so Paradoxical After All? Viewing the Privacy Paradox through Different Theoretical Lenses". Papers, 2014.
34. Y. Liu, J. K. Boyles, J. Genzer and M. D. Dickey. "Self-folding of polymer sheets using local light absorption". *Soft Matter*, vol. 8, pp. 1764-1769, 2012.
35. Kaplan, A. "Academia goes social media, MOOC, SPOC, SMOC and SSOC: The digital transformation of higher education institutions and universities". In: *Contemporary Issues in Social Media Marketing*. New York: Routledge, 2017. pp. 20-30.
36. I. Taylor, P. Walton and J. Young. "*The New Criminology: For a Social Theory of Deviance*". Routledge, Abingdon, 2013.
37. D. Boyd, S. Golder and G. Lotan. "Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. System Sciences (HICSS), 2010. 43rd Hawaii International Conference. IEEE, pp. 1-10, 2010.
38. E. Christofides, A. Muise and S. Desmarais. "Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes"? *Cyberpsychology and Behavior*, vol. 12, pp. 341-345, 2009.
39. O. Nov and S. Wattal. "Social Computing Privacy Concerns: Antecedents and Effects. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 333-336, 2009.
40. S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao and S. J. Upadhyaya. "Internet and online information privacy: An exploratory study of preteens and early teens". *IEEE Transactions on Professional Communication*, vol. 52, pp. 167-182, 2009.
41. D. H. Shin. "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption". *Interacting with Computers*, vol. 22, pp. 428-438, 2010.
42. L. Casaló, C. Flavián and M. Guinalíu. "The impact of participation in virtual brand communities on consumer trust and loyalty: The case of free software". *Online Information Review*, vol. 31, pp. 775-792, 2007.
43. D. J. Kim, D. L. Ferrin and H. R. Rao. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents". *Decision Support Systems*, vol. 44, pp. 544-564, 2008.
44. T. Dinev and P. Hart. "Internet privacy concerns and their antecedents-measurement validity and a regression model". *Behaviour and Information Technology*, vol. 23, pp. 413-422, 2004.
45. M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen. "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements". *Requirements Engineering,* vol. 16, pp. 3-32, 2011.
46. N. K. Malhotra, S. S. Kim and J. Agarwal. "Internet users" information privacy concerns (IUIPC): The construct, the scale, and a causal model". *Information Systems Research*, vol. 15, pp. 336-355, 2004.
47. C. L. Miltgen and D. Peyrat-Guillard. "Cultural and generational influences on privacy concerns: A qualitative study in seven

European countries". *European Journal of Information Systems*, vol. 23, pp. 103-125, 2014.
48. E. Hargittai and D. Boyud. "Facebook privacy settings: Who cares"? *First Monday*, vol. 15, no. 8, pp. 15, 2010.
49. A. L. Young and A. Quan-Haase. "Privacy protection strategies on Facebook: The Internet privacy paradox revisited". *Information, Communication and Society*, vol. 16, pp. 479-500, 2013.
50. L. S. Aeschlimann, R. Harasgama, F. Kehr, C. Lutz, V. Milanova, S. Müller, P. Strathoff and A. Tamò. "Re-Setting the Stage for Privacy: A Multi-Layered Privacy Interaction Framework and its Application". Mensch und Maschine Symbiose oder Parasitismus? Schriften der Assistierenden der Universität St.Gallen, 2014.
51. L. V. Casalo, C. Flavián and M. Guinalíu. "The role of security, privacy, usability and reputation in the development of online banking". *Online Information Review*, vol. 31, pp. 583-603, 2007.
52. A. J. Kim and E. Ko. "Do social media marketing activities enhance customer equity? An empirical study of luxury fashion brand". *Journal of Business Research*, vol. 65, pp. 1480-1486, 2012.
53. S. Bandyopadhyay, V. Shaw, A. Banerjee and D. Nag. "Social knowledge management: Use of social media for disseminating informal wisdom of elderly to the youth". *International Journal of Knowledge, Innovation and Entrepreneurship*, vol. 1, pp. 107-115, 2013.
54. Al-Hujran, O., M. M. Al-Debei, A. Chatfield and M. Migdadi. "The imperative of influencing citizen attitude toward e-government adoption and use". *Computers in Human Behavior*, vol. 53, pp. 189-203, 2015.
55. M. A. Perales, E. K. Drake, N. Pemmaraju and W. A. Wood. "Social media and the adolescent and young adult (AYA) patient with cancer". *Current Hematologic Malignancy Reports*, vol. 11, pp. 449-455, 2016.
56. E. W. Ngai, S. S. Tao and K. K. Moon. "Social media research: Theories, constructs, and conceptual frameworks". *International Journal of Information Management*, vol. 35, pp. 33-44, 2015.
57. K. Chai, V. Potdar and T. Dillon. "Content Quality Assessment Related Frameworks for Social Media. "*International Conference on Computational Science and Its Applications*". Springer, Berlin, pp. 791-805, 2009.
58 Warkentin, M., A. C. Johnston, E. Walden and D. W. Straub. "Neural correlates of protection motivation for secure IT behaviors: An fMRI examination". *Journal of the Association for Information Systems*, vol. 17, no. 3, p. 194, 2016.
59. X. Wang, C. Yu and Y. Wei. "Social media peer communication and impacts on purchase intentions: A consumer socialization framework". *Journal of Interactive Marketing*, vol. 26, pp. 198-208, 2012.
60. Z. Liu, Q. Min, Q. Zhai and R. Smyth. "Self-disclosure in Chinese micro-blogging: A social exchange theory perspective". *Information and Management*, vol. 53, pp. 53-63, 2016.
61. M. E. Keim and E. Noji. "Emergent use of social media: A new age of opportunity for disaster resilience". *American Journal of Disaster Medicine*, vol. 6, pp. 47-54, 2011.
62. A. M. Kaplan and M. Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media". *Business Horizons*, vol. 53, pp. 59-68, 2010.
63. N. Dabbagh and A. Kitsantas. "Personal learning environments, social media, and self-regulated learning: A natural formula for connecting formal and informal learning". *The Internet and Higher Education*, vol. 15, pp. 3-8, 2012.
64. A. Sarker, K. O'Connor, R. Ginn, M. Scotch, K. Smith, D. Malone and G. Gonzalez. "Social media mining for toxicovigilance: Automatic monitoring of prescription medication abuse from Twitter". *Drug Safety*, vol. 39, pp. 231-240, 2016.
65. A. E. Marwick and D. Boyd. "Networked privacy: How teenagers negotiate context in social media". *New Media and Society,* vol. 16, pp. 1051-1067, 2014.