Pacific Asia Journal of the
Association for Information Systems

ISSN 1943-7544

Research Paper doi: 10.17705/1pais.14401 Volume 14, Issue 4 (2022)

Privacy and Online Social Networks: A Systematic Literature Review of Concerns, Preservation, and Policies

Damion R. Mitchell[1,*], **Omar F. El-Gayar**[2]

[1,*]Dakota State University, United States, damion.mitchell@trojans.dsu.edu
[2]Dakota State University, United States, omar.el-gayar@dsu.edu

Abstract

Background: *Social media usage is one of the most popular online activities, but with it comes privacy concerns due to how personal data are handled by these social networking sites. Prior literature aimed at identifying users' privacy concerns as well as user behavior associated with privacy mitigation strategies and policies. However, OSN users continue to divulge private information online and privacy remains an issue. Accordingly, this review aims to present extant research on this topic, and to highlight any potential research gaps.*

Method: *The paper presents a systematic literature review for the period 2006 - 2021, in which 33 full papers that explored privacy concerns in online social networks (OSN), users' behavior associated with privacy preservation strategies and OSN privacy policies were examined.*

Results: *The findings indicate that users are concerned about their identity being stolen, the disclosure of sensitive information by third-party applications and through data leakage and the degree of control users have over their data. Strategies such as encryption, authentication, and privacy settings configuration, can be used to address users' concerns. Users generally do not leverage privacy settings available to them, or read the privacy policies, but will opt to share information based on the benefits to be derived from OSNs.*

Conclusion: *OSN users have specific privacy concerns due primarily to the inherent way in which personal data are handled. Different preservation strategies are available to be used by OSN users. Policies are provided to inform users, however, these policies at times are difficult to read and understand, but studies show that there is no direct effect on the behavior of OSN users. Further research is needed to elucidate the correlation between the relative effectiveness of different privacy preservation strategies and the privacy concerns exhibited by users. Extending the research to comparatively assess different social media sites could help with better awareness of the true influence of privacy policies on user behavior.*

Keywords: Privacy Concerns, Privacy Policies, Online Social Networks, User Behavior, Privacy Preservation Strategies.

This research article was submitted on Nov-2021 and under four revisions, accepted on June-2022.

Citation: Mitchell, D. R., & El-Gayar, O. F. (2022). Privacy and Online Social Networks: A Systematic Literature Review of Concerns, Preservation, and Policies. *Pacific Asia Journal of the Association for Information Systems, 14*(4), 1-25. https://doi.org/10.17705/1pais.14401

Copyright © Association for Information Systems.

Introduction

Boyd and Ellison (2007) define Online Social Networks (OSN) as a web-based service that allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. OSNs have become a typical cultural spectacle for millions of Internet users not only as a form of entertainment, but also for information sharing. OSNs such as Facebook, Instagram, Twitter, and LinkedIn all play important roles in the lives of many daily. Social media sites are one of the most used Internet services worldwide (Boyd & Ellison, 2007). In 2020, over 3.6 billion people were using social media worldwide, a number projected to increase to almost 4.41 billion in 2025 (Tankovka, 2021b). Facebook at the end of the first quarter of 2021 had an estimated 2.85 billion active users, making it the largest social network worldwide (Tankovka, 2021a).

With their ubiquity, OSNs present threats to privacy due to their inherent handling of personal data (Cutillo et al., 2009). Privacy has long been of interest to researchers in several disciplines; with many definitions of privacy including the same basic concept: control over the use (particularly the secondary use) of one's information (Belanger & Crossler, 2011; Mason, 1986). In a survey by Raine (2018) it was shown that 91% of Americans agreed that most individuals have lost control over the collection and use of their personal information by online companies; this has affected the trust that these users exhibit. For example, after the data breach at Facebook, a survey by Perrin (2018), found that 25% of users on Facebook, deleted their accounts. Privacy can be viewed from the standpoint of control; whether it is control over personal data, the choice to disclose data, the number of friends present in disclosure, or controlling which persons to discuss and share issues with (Mitchell & El-Gayar, 2020). Fundamentally, privacy involves the ability of an individual to control the disclosure and use of one's personal information.

However, there is no universal definition for users' privacy concerns. In general, it refers to the "degree to which an individual perceived a potential for a loss associated with personal information" (Pavlou, 2011, p. 981). Further, Fletcher and Peters (1997) shared that privacy concern measures the degree of control by users over the personally identifiable information. Several studies have conceptualized privacy concerns as general concerns that show individuals' fundamental worries about possible deprivation of information privacy (Malhotra et al., 2004). Smith and Milberg (1996) conducted a study to understand the complexity of users' privacy concerns, from which four dimensions were presented to include: collection, unauthorized secondary use, improper access, and errors. Therefore, when users have high levels of privacy concerns, they may desist from sharing personal information or in some cases to submit fake information (Acquisti & Gross, 2006). Prior studies have shown that online privacy concerns significantly influence perceived trust and risk notions (Kansal, 2014; H. Smith et al., 2011), as well as for protection behavior—the willingness to disclose online information (T. Wang et al., 2016).

When users express privacy concerns, they invariably would want to know what strategies can be used to reduce them. Privacy preservation strategies are the techniques with which individuals safeguard their information and mitigate potential privacy breaches (Young & Quan-Haase, 2013). For example, Oomen and Leenes (2008) distinguished three dimensions of strategies that users may employ to protect their privacy, with the first being behavioral strategies such as using anonymous emails; secondly, well known security measures such as spam filters, and thirdly, advanced strategies such as trust certificates. In another study, M. Wang et al. (2016) explained that privacy protection strategies can be seen as a type of access authorization management. Other studies have been done to investigate the online privacy concerns of users and the strategies they use to mitigate these concerns (Quan-Haase & Ho, 2020). However, for strategies to be effective, users will need to proactively adopt them.

https://aisel.aisnet.org/pajais/vol14/iss4/1
DOI: 10.17705/1pais.14401

Within the realm of protecting a user's privacy, privacy policies are said to be statements or legal documents that disclose some or all of the ways a party gathers, uses, discloses and manages customer or client data (L. Wang et al., 2019). Prior research have accentuated the role of privacy policies in trust building in other contexts, such as online shopping, website registration, and mobile Internet use (Capistrano & Chen, 2015). The presence of a robust website privacy policy enhances online shoppers' trust, and, in turn, reduces their privacy concerns (Rifon et al., 2005). When a privacy statement is clearly presented by websites, consumers are more willing to read it carefully to attain more online services (Steinfeld, 2016). However, privacy policies that are meant to address privacy concerns are often lengthy, legally worded documents written to protect the provider (Barth & de Jong, 2017). It is also claimed that users essentially never read the Terms of Service of service providers, and generally have no direct knowledge of their privacy policies (Obar & Oeldorf-Hirsch, 2020).

With the proliferation of privacy-related research and the heightened awareness of the threats to privacy, a need exists to review and assess the current state of research as it pertains to evolving users' privacy concerns, users' behavior regarding various privacy preservation strategies and privacy policies. Accordingly, this study presents a Systematic Literature Review (SLR) and Analysis of Research pertaining to privacy and OSN; to include the privacy concerns of OSN users, strategies to protect users' privacy, and to understand how OSN privacy policies relates to users' privacy behavior. The aim of this review is to present extant research on this topic, and to highlight any potential research gaps. Specifically, the SLR addresses the following questions:

1. What are the main privacy concerns of OSN users discussed in the literature?
2. What are the major OSN privacy preservation strategies investigated?
3. What are the OSN privacy policies related issues presented in the literature?

This paper is organized as follows. The next section describes the review method used to extract, analyze, and synthesize the selected studies followed by the result of analyzing the 33 identified primary studies and summarizes their findings based on the research questions. Next, we provide a discussion on the results based on each research question. The final section provides a conclusion and the limitations associated with the study.

Methodology

A Systematic Literature Review methodology (Liberati et al., 2009) was utilized to identify peer-reviewed articles from electronic databases which contained research that examined the privacy concerns associated with OSN users, strategies to mitigate these concerns, and the relation of OSN privacy policies on the users' behavior. We chose a systematic literature review because it is a "systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners" (Fink, 2010, p. 3). In other words, a systematic review attempts to collate all empirical evidence that fits pre-specified eligibility criteria to answer a specific research question. It uses explicit, systematic methods that are selected with a view to minimizing bias, thus providing reliable findings from which conclusions can be drawn and decisions made (Oxman & Guyatt, 1993).

Data Sources and Search Strategies

The research articles used in this systematic literature review were obtained through an extensive search of relevant databases: ACM Digital Library, IEEE Xplore, AIS eLibrary, Web of Science and ABI/Inform. These were selected based on their relevancy to the Information Systems domain, dealing with areas such as security, privacy, social, and behavioral sciences. Furthermore, these databases were selected because they are broad and the studies published are peer-reviewed, which provides a quality check of primary studies. In addition, they represent some of the leading databases used by Information Systems researchers; as such all results that appeared in these databases were considered. The search terms include the keywords related to privacy concerns, preservation strategies, or privacy policies in the context of online social networks. Costa and Monteiro (2016) indicated that the selection of keywords is a critical step in any systematic review as it determines which articles are to be retrieved. The period selected for this study ranged from 2006 - 2021. This period was selected as most of the work that deals with OSN occurred after 2005, as confirmed from the databases searched. The criteria that the search string must appear in the title or abstract was followed strictly. The articles that were critically analyzed in this review study met the inclusion and exclusion criteria described in Table 1.

Table 1 - Inclusion and Exclusion Conditions Used

Criteria	Conditions
Inclusion	Search strings should appear in title or abstract of the paper The language of the paper must be English The paper should identify OSN users' concerns or discuss the behavior of OSN users towards their privacy concerns The paper should discuss the behavior of OSN users in relation to privacy preservation strategies The paper should discuss the behavior of OSN users in relation to privacy policies Full-Text Papers
Exclusion	Poster presentations, books, conference panels and summaries, review papers, and research in progress papers. Papers published on unrelated topics such as crime, politics etc.

Quality Assessments

According to Al-Emran et al. (2018) one of the significant factors that needs to be observed along with the inclusion and exclusion criteria is the quality assessment. A quality checklist adapted from Kitchenham and Charters (2007) was used in order to gather evidence related to the research questions in order to make judgement on the quality of papers. By quality appraisal of each primary study, we could determine the reliability of the sources and select quality studies prior to synthesis of results. The study quality checklist consists of four general questions to measure the quality of selected studies as shown in Table 2.

Table 2 - Quality Assessment Checklist

#	Question
SQ1	Are the research aims clearly specified?
SQ2	Is the method of analysis appropriate and adequately explicated?
SQ3	Are the data collection methodologies sufficiently detailed?
SQ4	Does the study add to your knowledge or understanding?

Each publication was measured according to the following ratio scale: Yes = 1 point, No = 0 point, and Partially = 0.5 point. The quality assessment was performed independently by two authors, and discrepancies were discussed until an agreement was reached. The inter-rater agreement (kappa) between the two authors was used to assess the degree of agreement (Landis & Koch, 1977)

Results

We identified 841 studies that contained search string keywords in their titles or abstracts. The papers identified in the identification phase were screened to remove duplications that excluded 107 studies. The exclusion criteria were applied to 841 papers that reduced the total

https://aisel.aisnet.org/pajais/vol14/iss4/1
DOI: 10.17705/1pais.14401

count to 734 papers. The titles and abstracts of 734 papers were analyzed to determine their relevance that made us exclude 555 papers. A total count of 179 studies comprises the final phase. The full text of the remaining 179 studies were examined in greater detail. By applying the inclusion criteria, 147 papers were discarded resulting in 33 papers included in the final review. Figure 1 shows the flow of information through the different phases of the systematic literature review.

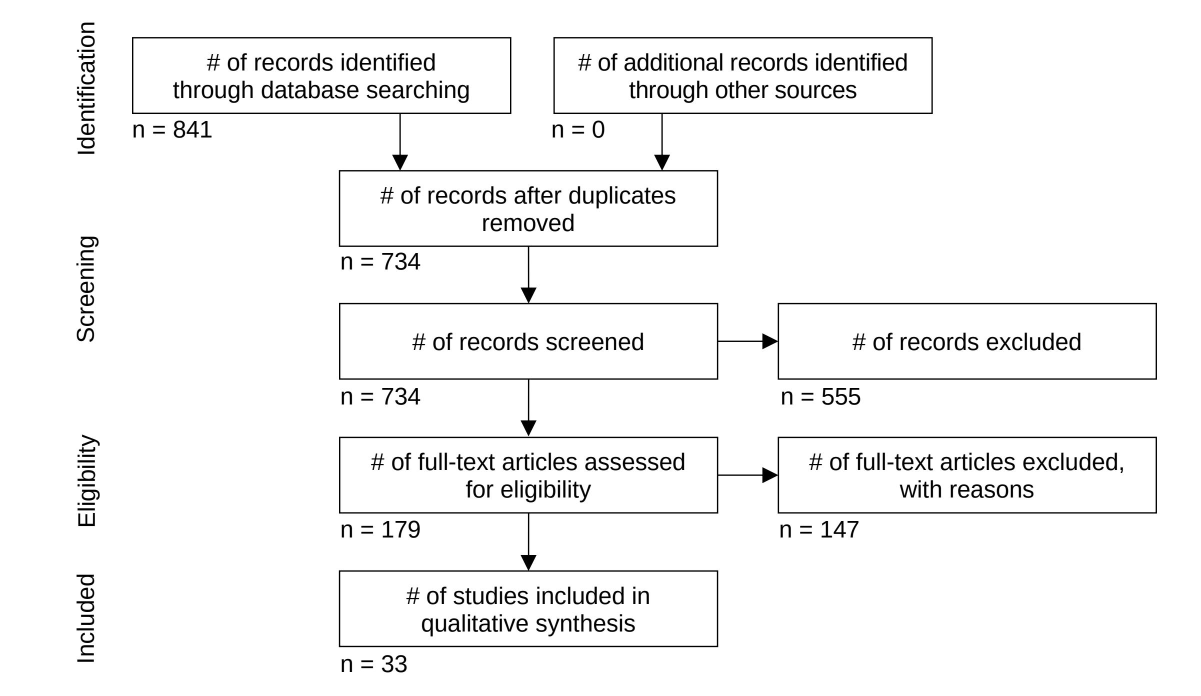
Identification
# of records identified through database searching
n = 841
# of additional records identified through other sources
n = 0
Screening
# of records after duplicates removed
n = 734
# of records screened
n = 734
# of records excluded
n = 555
Eligibility
# of full-text articles assessed for eligibility
n = 179
# of full-text articles excluded, with reasons
n = 147
Included
# of studies included in qualitative synthesis
n = 33

Figure 1 - Phases of the Systematic Review (Liberati et al., 2009)

The results obtained from each database are shown in Figure 2.

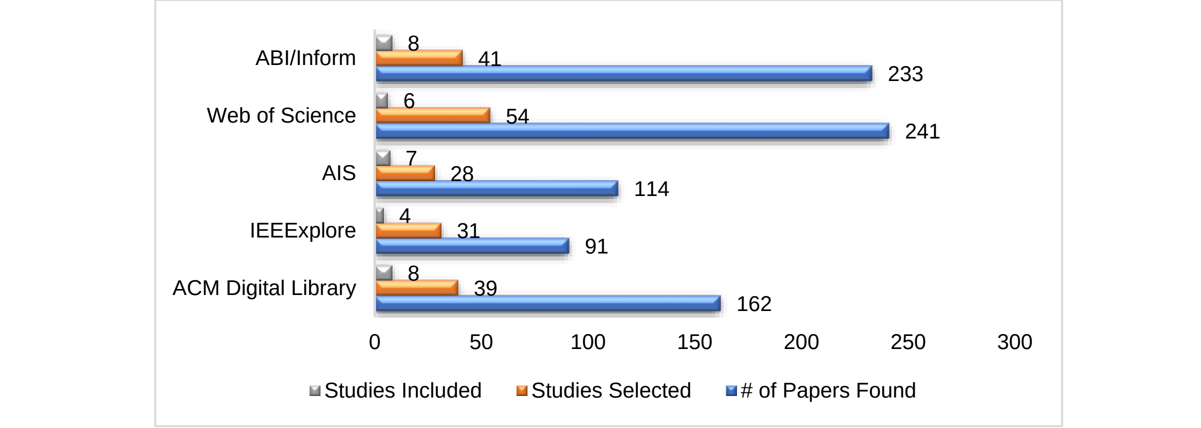

Figure 2 - Number of Primary Papers Selected

Table 3 shows the summary of the quality scores for all identified articles, where the quality of 21 articles (64%) and 10 articles (30%) were classified as very good and good respectively, while 2 articles (6%) were assessed as fair. None of the articles was denoted as 'very poor' quality score; therefore all 33 selected articles were included for further analysis. The inter-rater agreement (kappa) between the two authors was substantial (kappa = .82) which, according to Landis and Koch (1977), indicates almost perfect agreement between the assessments performed by the two authors.

Table 3 - Quality Scores

Quality Score	Very Poor (0 - < 1)	Poor (1 - <2)	Fair (2 - <3)	Good (3 - <4)	Very Good (4)	Total
Number of Studies	**0**	**0**	**2**	**10**	**21**	**33**
Percentage (%)	**0%**	**0%**	**6%**	**30%**	**64%**	**100%**

The publication year of each primary study was tabulated, from which it showed that studies published on this topic began to appear in the databases after 2005. Figure 3 shows the trend of publication over the years based on the 33 selected papers with 2010 and 2013 accounting for most of the papers. It also highlights the average quality assessment measurement over time, which suggests that papers have been generally very good based on the established metrics.

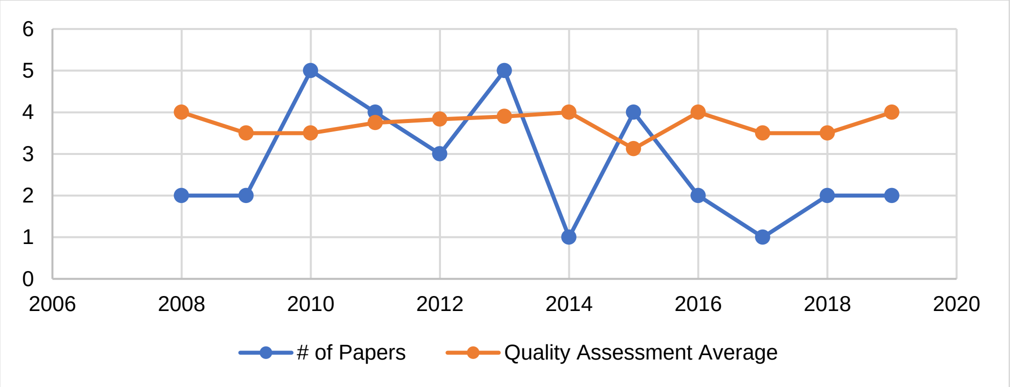

Figure 3 - Number of Primary Papers Distributed by Year

Privacy Concerns Associated with OSN Users

The acceptance and usage of OSNs have transformed many individuals' lives in terms of how they form and shape social relations. This growth has presented several concerns, principal of which is that of privacy. Based on the varying conceptualizations of privacy concerns, the concept map shown in Figure 4, gives support for Pavlou (2011) idea of probable loss of personal information which may occur in areas such as data leakage and through Third-Party applications. The findings are consistent with the conceptualization espoused by Smith and Milberg (1996) in which the concerns fell into at least one of the four domains: collection of personal information, unauthorized secondary use, improper access or errors pertaining to personal information. For example, Third-Party applications would fall under unauthorized secondary use while identity theft, under improper access. The concept of privacy is not a new phenomenon, but with the ubiquity of OSN, the SLR revealed varying privacy concerns as presented below.

Data Leakage

One of the privacy issues in OSNs is the abuse and leakage of profile and personal information in which the more posts made by users, is the more data that is available for potential misuse by malicious users (Ladan, 2015). Consequently, Krishnamurthy and Wills (2010) discovered from an examination of thirteen (13) OSN sites, that each leaked private information to tracking sites and in some cases to third-party applications. The data leakage included leakage of unique identifier of OSN users, and specific pieces of personal identifiable information. In another study, Krishnamurthy and Wills (2009) showed that OSNs consistently demonstrate leakage of user identifier information to one or more third-parties via Request-URIs, Referrer

https://aisel.aisnet.org/pajais/vol14/iss4/1
DOI: 10.17705/1pais.14401

headers and cookies. The notion of data leakage in OSN was expanded into two categories, information and location leakage (Ali et al., 2018). In essence, social media are all about openly sharing and bartering information with friends. Some users share even their health-related data, in which such delicate and sequestered content may have an undesirable implication for OSN users. With respect to location-leakage, OSN users tend to access social networks through mobile devices, which may encourage users to share their location information. Thus, the revealing of geographic data on social-networking sites may be used by attackers to harm users (Ali et al., 2018).

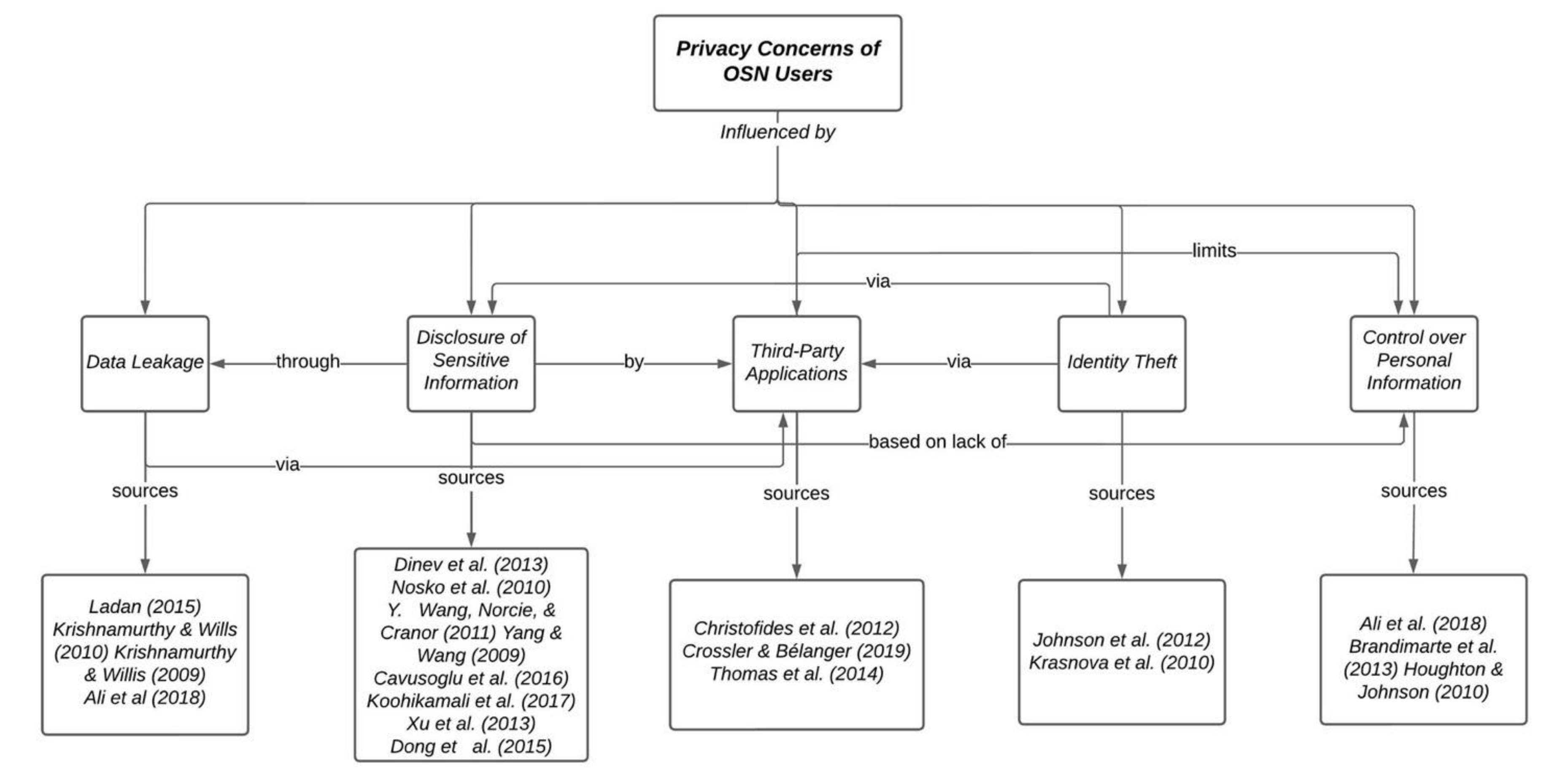
Privacy Concerns of OSN Users
Influenced by
limits
via
Data Leakage
through
Disclosure of Sensitive Information
by
Third-Party Applications
via
Identity Theft
Control over Personal Information
based on lack of
via
sources
sources
sources
sources
sources
Ladan (2015) Krishnamurthy & Wills (2010) Krishnamurthy & Willis (2009) Ali et al (2018)
Dinev et al. (2013) Nosko et al. (2010) Y. Wang, Norcie, & Cranor (2011) Yang & Wang (2009) Cavusoglu et al. (2016) Koohikamali et al. (2017) Xu et al. (2013) Dong et al. (2015)
Christofides et al. (2012) Crossler & Bélanger (2019) Thomas et al. (2014)
Johnson et al. (2012) Krasnova et al. (2010)
Ali et al. (2018) Brandimarte et al. (2013) Houghton & Johnson (2010)

Figure 4 - Concept Map of Privacy Concerns of OSN Users

Disclosure of Sensitive Information

Dinev et al. (2013) define information sensitivity as a “personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent” (p. 302). It was shown that information sensitivity increased the perceived risk of users. Consequently, information sensitivity and their disclosure also characterize a leading concern for OSN users (Y. Wang et al., 2011). Even though there is a potential for significant disclosure through OSN profiles, Nosko et al. (2010) demonstrated that people were displaying approximately 25% of possible information for other users to view, which could be deduced as a direct decision to limit the disclosure of sensitive information. Information sensitivity has been shown to contribute to the privacy concerns of users. This may occur through data leakage or by third-party applications. In addition, the disclosure of sensitive information may cause an unsuspecting OSN user’s identity to be stolen (Cavusoglu et al., 2016; Koohikamali et al., 2017; Xu et al., 2013). For example, Dong et al. (2015) showed that the sensitivity of the information and its appositeness along with the audience are important factors which influence information disclosure on OSN. Yang and Wang (2009) outlined that when the sensitivity level of requested information is high, users’ privacy concerns and behavioral intentions are impacted.

Third-Party Applications

Several OSNs provide an Application Programming Interface (API) for third-party developers to create applications that can be used on their platform. These applications give rise to a number of privacy concerns, due to the fact that codes are hosted outside of the OSN and ultimately the control of the users. Christofides et al. (2012) shared that these third-party applications can track social network users’ actions or grant access to advertisement associates for them to access and gather social network users’ data for commercial and advertising purposes. OSN users have little power over how their data are collected and used by OSN platform and its third-party affiliates (Crossler & Bélanger, 2019). Previous work has also conveyed that even though third-party applications are extensively used for nonthreatening purposes, they are frequently exploited by attackers to compromise many accounts for contemptable purposes such as propagating spam and malware on OSNs (Thomas et al., 2014).

Identity Theft

This occurs because OSNs contain several personally identifiable information such as real name, date of birth, and location (Y. Wang & Nepali, 2015). Furthermore, studies have shown that the most reported concern for OSN users is hinged on the prevalence of identity theft (Johnson et al., 2012; Krasnova et al., 2010). The findings showed that this type of attack to OSNs may originate from both inside and outside the network. This may occur when OSN users accept friend requests from unknown people, share account details with others, or click on links that lead to other websites.

Control Over Personal Information

Many OSN users are concerned that they have inadequate control over their personal information stored by social media sites. Users want to be able to control when, how, and to what extent personal information is collected, used, and shared. Although OSNs provide a particular level of access control to data owners via customized settings, where certain contents can be hidden from unauthorized access, users are still skeptical as to whether the shared information are being kept private (Ali et al., 2018). In addition, Brandimarte et al. (2013) explained that individuals usually require more control over the release and accessibility of their information (i.e., if they are able to control which information will be published their willingness to disclose sensitive information will increase). Houghton and Joinson (2010) explained that OSN users are often unaware of, or at least isolated from the storage and utilization of their shared information, and that such ubiquitous data collection is considered harmful to personal privacy.

Strategies to Protect Users' Privacy

Several strategies have been presented to deal with users' privacy concerns. These are normally the techniques or tools with which individuals safeguard their information and lessen possible privacy breach; these tactics are summarized in the concept map shown in Figure 5.

Authentication

To achieve confidentiality, privacy, and access control it must be possible to authenticate users and attribute messages to the users who sent them. For instance, Facebook attempts to guard their users by adding authentication methods such as CAPTCHA to guarantee that the registered user is a real person (Boshmaf et al., 2011). Additionally, where possible, OSN users should activate secure browsing, and any other possible authentication methodologies such as two-factor authentication. L. Wang et al. (2019) recommended that the adoption of multiple layers of firewalls protection can also be used to lower the privacy risks of the users.

Encryption (Cryptography)

Social media platforms are affected by thousands of attacks each second, and at the systems level to decrease the impact of wrong choices on the user's part, the data should be protected using cryptographic keys which may be computationally expensive, to defend against things such as impersonation or phishing attack (Franchi et al., 2015). OSN sites such as Facebook and Twitter have employed Secure Socket Layer (SSL) technology to encrypt their users' personal data. Consequently, as the basis for integrity, enhanced encryption tools can also be used by OSN users to afford confidentiality and in some instance to protect aspects of their profile and instant messages shared using these platforms (Barghuthi & Said, 2013).

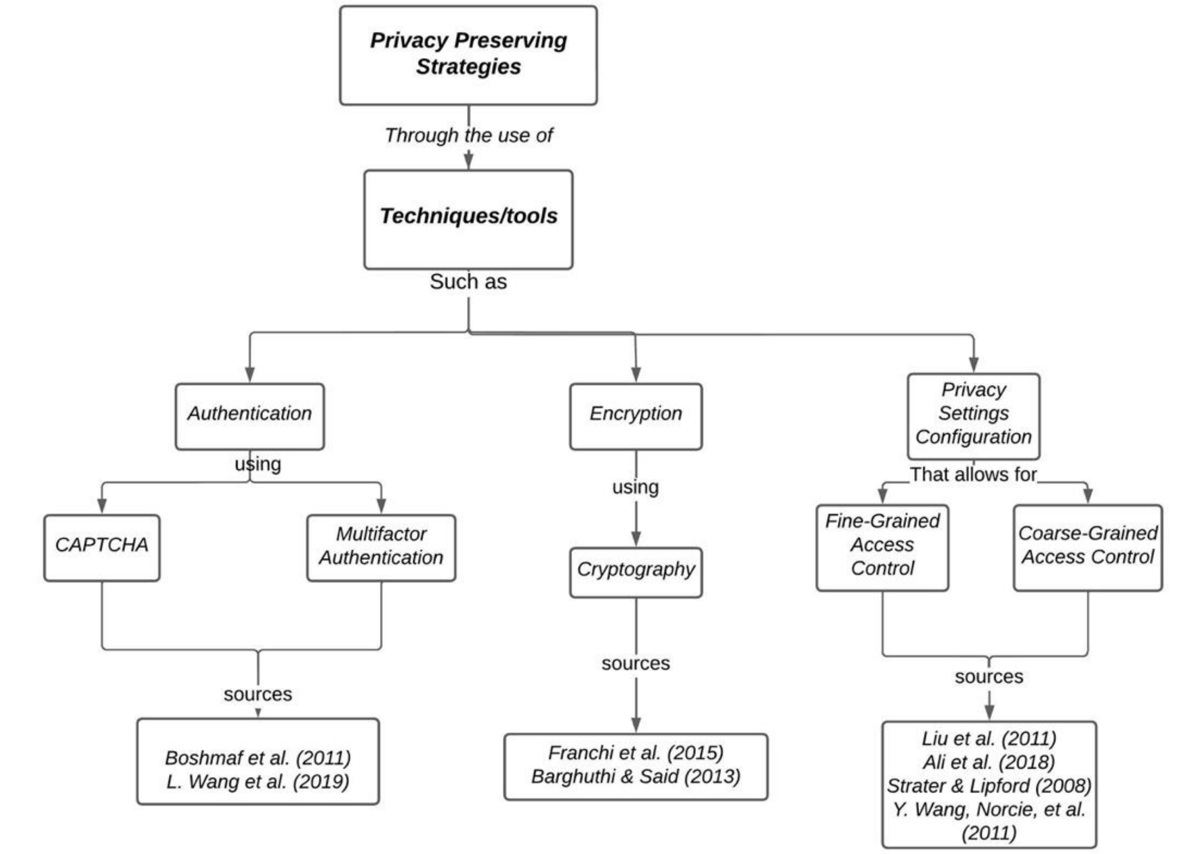

Figure 5 - Concept Map of OSN Users Privacy Preserving Strategies

Privacy Settings Configuration

Privacy settings are useful when seeking to alleviate problems of unauthorized data access by other users and providing the ability of users to conceal information from a friend or group. Studies have revealed that users on OSNs often do not take advantage of privacy settings available to them. When OSN users refuse to change their privacy settings, they tend to be more open than would be desired (Liu et al., 2011). Generally, the usage of privacy settings by OSN users is for their own convenience. Many OSNs support several configurable user privacy settings that enable users to protect their personal data from other users or applications. Strater and Lipford (2008) argued that users are confused by the existing and extensive privacy settings and are not utilizing them to customize their information accessibility to certain audiences. Y. Wang et al. (2011) showed that while some users are aware of the available privacy settings, some reportedly checked their settings occasionally, and a few, regularly. Consequently, OSN users are encouraged to keep personalized privacy settings and take full advantage of the privacy-protection techniques provided by their OSNs. Similarly, users are guided to regularly revise their privacy settings to be more restrictive, because several OSNs modify their privacy settings after every update (Ali et al., 2018).

Privacy Policies and OSN

The concept map presented in Figure 6 summarizes the OSN privacy policies related issues.

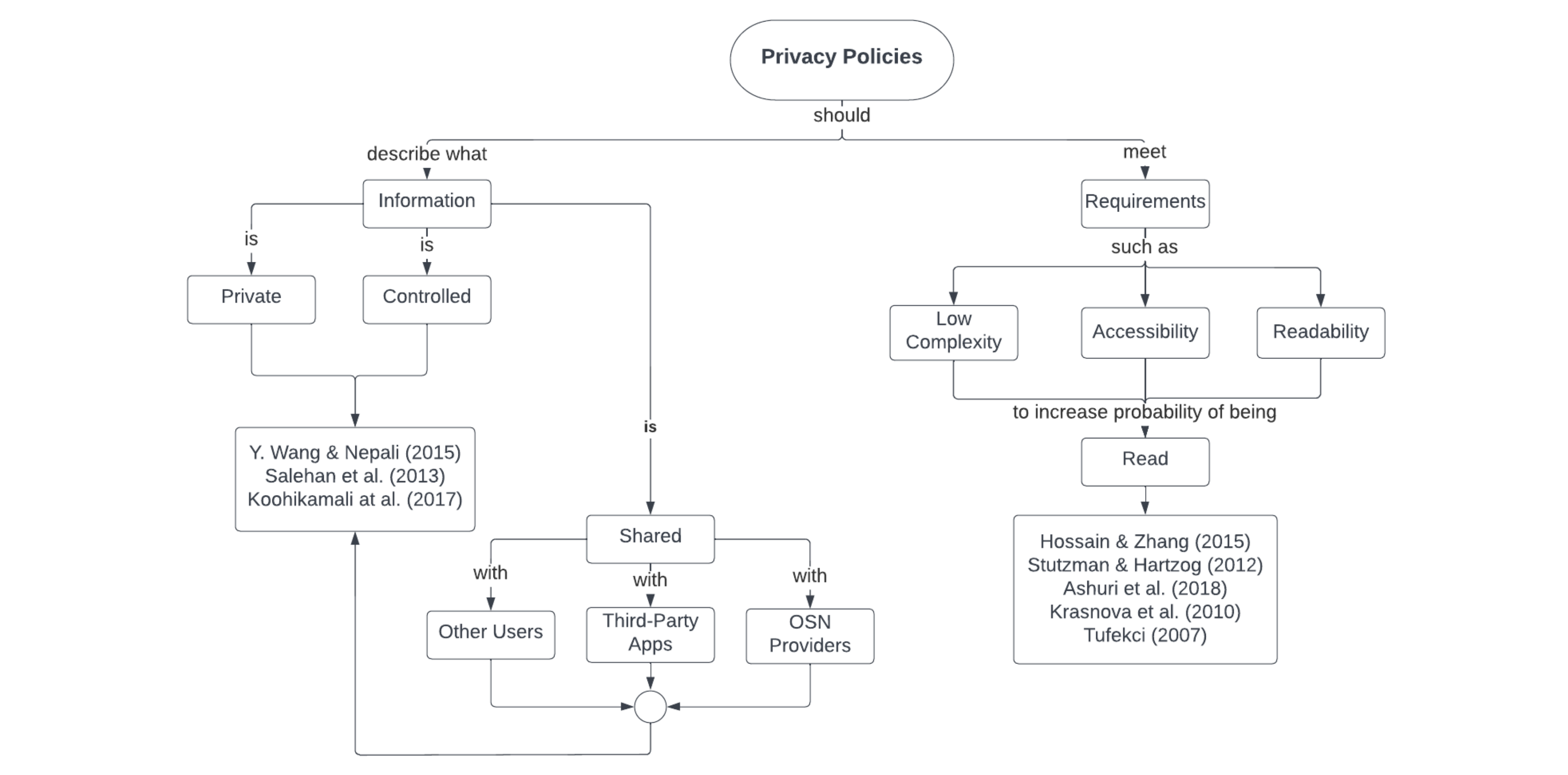

Figure 6 - Concept Map of OSN Privacy Policies

OSN privacy policies describe what information is private, how the data is shared, how users can control the way OSN providers use their information and create an agreement between the social networking site and its users (Y. Wang & Nepali, 2015). A key behavior of OSN users is based on information sharing, which can be connected to the frequency of the information sharing behavior or the level of online private information disclosure (Salehan et al., 2013). Researchers investigated how OSN users' behaviors are impacted by the privacy policies of these networks. Hossain and Zhang (2015) conducted a study which showed that most respondents were worried to varying degrees about their online privacy, but not all these users have read the privacy policies of their OSNs. This highlights the dichotomy that exists between stated privacy concerns and the actual behavioral response (Stutzman & Hartzog, 2012; Tufekci, 2007). Furthermore, research studies find that there is a probability that if a social networking site has its privacy policy then people tend to share more information on that site (Koohikamali et al., 2017). On the contrary, privacy policy is linked with limited information disclosure in Facebook based on the amount of time required to read them (Ashuri et al., 2018; Koohikamali et al., 2017). This was supported by Krasnova et al. (2010) who disclosed users will reduce the amount of information divulged in response to their privacy concerns. While other OSN users take an all-or-nothing approach when releasing personal information, regardless of their knowledge of the privacy policies.

Discussion

The purpose of this study was to systematically review prior research on the privacy concerns associated with OSN, the suggested strategies to address these concerns, and the privacy policy related issues of OSN users. Overall, the results provide strong evidence for research addressing the three questions of interest that pertain to privacy concerns, OSN privacy preservation strategies, and OSN privacy policies. With respect to the first research question concerning OSN users' privacy concerns, the findings point to the prevalence concerns regarding disclosure and control of sensitive information. Data leakage particularly through third-party has also been identified. Only two articles directly addressed concerns with identity theft. Studies pertaining to the second research question regarding preservation strategies emphasized user behavior and efficacy of the configuration of privacy settings. Other strategies addressed, were authentication and encryption. Last but not least, studies addressing the third research question pertaining to OSN privacy policy related issues highlighted concerns with complexity, accessibility, and readability of said policies. Others emphasized the relation between the impact of policies and information sharing behavior. The following sub-sections provide an in-depth discussion with respect to each of the research questions.

Privacy Concerns

When OSN users have significant privacy concerns, this may introduce a feeling of not having control over personal information. This will result in apprehensions as to whether the OSN providers have the competence and veracity to ensure information privacy. The findings show that while users have expressed major concerns over identity theft through OSNs, users also are burdened about the possible losses related to information leakage and abuse. This is in line with findings of other studies (Deliri & Albanese, 2015; Fire et al., 2014) regarding the concern of OSN users on how their private information is gathered by opponents with the intention of impersonating them, primarily through the use of phishing. Additionally, most users are vulnerable to having their OSN identity information leaked via mechanisms like tracking cookies. A solution to the problem of privacy leakage trigged by OSN users' behavior, has seen researchers implementing a series of access-control methodologies aligned with OSNs (Wu & Pan, 2021).

Results also show, that with a plethora of third-party applications associated with OSNs, users are generally concerned in terms of their lack of knowledge as to what exploitations may occur through these systems. Privacy concerns for users were generally context-related, where users were far more positive to disclose sensitive information for the purpose of product improvement, but more reluctant when the transfer included third parties (Matt et al., 2019). In a study conducted by Kshetri (2011), it was shown that cybercrimes which target social network users are generally facilitated by the proliferation of third-party applications in which some are designed to steal personal information. This is confirmed in a review by Beye et al. (2010) in which it was highlighted that based on the wealth of information stored on OSN, it is of great value to third-parties both private and commercial who may use various techniques unknowing to the users to capture their data. For example, in a recent occurrence, it was conveyed that both public and private profile data of millions of Facebook users were garnered through a mobile application by Cambridge Analytica for political purposes (Cadwalladr & Graham-Harrison, 2018). A study by Egele et al. (2015) also confirms that third-party applications are frequently used to send malicious messages. We propose that users uninstall third-party applications that may be collecting unauthorized data, as some of them may be malicious and may gain full access to user's profile and the data being shared. Conversely, Zhang et al. (2020) indicated that perceived third-party assurance has a significant influence on online customer trust, which implies that providing third-party assurance to users can be utilized to reduce privacy concerns and thereby promote trust.

Another finding showed that privacy concern also reflects a user's trepidation on information disclosure, especially when it comes to sensitive personal identifiable data. It is apparent that users' privacy concerns and behavioral intentions are affected negatively when the sensitivity of the information being requested by the OSN providers is deemed to be high. This is supported by Sun et al. (2019), however, it was also shown that when users perceive that benefits can be derived their behavior of information disclosure is positively influenced.

Privacy Preserving Strategies

Privacy is generally a major concern of OSN users, for which several strategies have been proposed to address these concerns. The findings demonstrate that one of the fine-grained approaches recommended for users of these systems is to appropriately adjust the privacy settings which are provided by these sites to help protect an individual's user data. This is confirmed by other studies (Fire et al., 2014; Kayes & Lamnitchi, 2017) where users are encouraged to use this fine-grained approach for privacy management. On the other hand, OSN providers should have easy to use privacy setting functions which provide for coarse-grained access control. We recommend that users who are not confident in terms of how to adequately adjust these settings, should minimize the information shared on these platforms to protect their privacy. The result also showed that the strategy of having robust encryption and authentication mechanisms must be implemented at both the OSN providers' and users' levels to further ensure the privacy of the personal information shared on these sites. This finding is in line with other studies where the legitimacy of OSN is ensured through authentication procedures such as CAPTCHA, multi-factor authentication, and photos-of-friend identification. The studies also showed that the use of appropriate encryption scheme can provide better privacy protection in OSNs.

Privacy Policies on OSN

A crucial aspect of information sharing is where OSNs seek to meet the expectation about privacy protection as expressed by users. OSN privacy policies should offer the users a straightforward and flexible way to apprise and enforce their privacy preferences to other users, to third parties and to the OSN service providers. In essence, users must be given the assurance that privacy policies are highly accessible (Hidayanto et al., 2013). Consequently, privacy policies and other privacy preserving mechanisms must address the issues of how to prevent the misuse of user information. The findings show that when users are acquainted with the privacy policies and especially how their information will be shared, the revelation of personal information was more likely. This contradicts the findings of Fiesler and Bruckman (2014) where it is shared that generally people do not read the privacy statements and when they do, they do not understand them. For instance, users may consider the cost of reading intricate privacy policies in their entirety overshadows the dangers, deciding that the benefits of using a service outweighs any potential privacy abuse concerns (Flender & Müller, 2012).

Another result showed that many users who generally do not review the policies, deemed them to be long and laborious; this results in the users' lack of knowledge, which may have a negative impact on their actual behavior. This is confirmed by prior researchers who have presented readability, format, use of legal jargon, special expressions, and specialized language in the creation of privacy policies as a deterrent to reading by many users (Milne & Culnan, 2004; Tsai et al., 2011). Therefore, since the policies are not documented in a manner easily understandable by the average, non-expert user, the OSN provider can modify them without the users noticing it, thus putting the users at great risk of privacy violations (Dwyer et al., 2007). A data privacy risk arose where user's lack of confidence in the privacy policy and their apprehensions about data sharing practices were voiced as major privacy concerns (Prakash & Das, 2020).

Users may be inclined to review privacy policies if they are presented by default and may devote significant time to reading it. This would suggest that the minimum requirements for privacy policies should include low complexity, accessibility, high comprehensiveness, and readability. While OSN users may not read the privacy policies, they may opt to share personal information based on the benefits to be derived from these social media sites even with demonstrated privacy concerns. There is a dichotomy that exists between the articulated concerns of OSN users about their privacy, while on the other hand they do nothing to address them. This disregard of policies is extensively denounced and often held up as a quintessential example of the "privacy paradox", whereby users who claim to be concerned about privacy still show minimum regard for it in practice (Norberg et al., 2007).

Future Research

With respect to the pertinent body of literature, the findings of the review indicate that further studies may find it necessary to examine the individual user's expressed privacy concerns over time through a longitudinal study. Additionally, research can be done to examine users' attitude toward privacy and the contributing factors that motivate them to share information on these OSN platforms. Research could further explore privacy-related behavior such as privacy paradox in the context of OSNs and as it pertains to various perspectives, e.g., healthcare and user groups, e.g., by gender or age. Furthermore, research may compare the behavior of users from select OSNs as influenced by the privacy policies of individual providers. Additional studies can be conducted to ascertain whether users' privacy behaviors on OSN are similar to that of using websites for online shopping. Moreover, case studies can be advanced in seeking to answer the question of how privacy-preserving applications are used by OSN users. This could be supplemented by examining the correlation between different privacy preserving approaches and the overall privacy concerns exhibited by users.

It is worthwhile noting that the systematic literature review, although extensive, may have overlooked some relevant studies owing to the limitations of the scientific databases, specific keywords employed in the search, and timeframe selected for this review. Furthermore, divergent types of studies such as practitioner articles, government reports, and policy documents are not included. Future reviews may broaden the scope to emphasize an industry and government perspective.

Conclusion

OSNs such as Facebook, Instagram, Twitter, and LinkedIn all play important roles in the lives of many daily; with it comes specific privacy concerns due primarily to the inherent way in which personal data are handled. In this study, a systematic literature review of 33 papers from five databases published between 2006 and 2021 was conducted to understand research trends on privacy related concerns for OSN users, user behavior associated with strategies that can be utilized to protect users' privacy, and to explore the relation of privacy policies on the information sharing behavior of OSN users. Our findings unearthed major privacy concerns expressed by users such as data leakage, information sensitivity, third-party applications, data control and identity theft. Due to the myriad privacy concerns, strategies such as privacy setting configurations, authentication, and encryption (cryptography) have been implemented or used to mitigate these concerns. OSN privacy policies should offer the users an upfront and flexible way to apprise and apply their privacy preferences to other users, to third-parties and to the OSN service providers. However, these policies at times are difficult to read and understand, but studies show that there is no direct effect on the information sharing behavior of OSN users, as a dichotomy exists between the expressed privacy concerns and the actual behavioral response.

From the theoretical perspective, this study makes important contributions to the privacy literature by systematically analyzing evidence from research and by providing an integrated view of privacy concerns of OSN users. The study also highlights user behavior associated with privacy preserving strategies that can help researchers to conduct a detailed study on the relationships of these techniques and which combinations can provide users with the best privacy protection. Practically, the findings from this study can assist policy makers in understanding the key privacy concerns of OSN users, and proactively implement policies to address these concerns. The research findings could help practitioners in introducing improvements in existing OSN platforms by understanding users' behavior towards OSN privacy policies. In addition, OSN providers will have a better understanding of how the expressed privacy concerns among users can affect usage of these OSN platforms. This can further actuate practitioners to present other privacy preserving techniques to the OSN providers.

In general, in the modern era of information technology, online privacy continues to be an area of interest for users. Therefore, having an appreciation of OSN users' behavior toward privacy concerns, the preservation strategies available, and the role of privacy policies are important.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.

Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2018). Technology Acceptance Model in M-learning context: A systematic review. *Computers & Education*, *125*, 389-412.

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. (2018). Privacy and security issues in online social networks. *Future Internet*, *10*(12), 114.

Ashuri, T., Dvir-Gvisman, S., & Halperin, R. (2018). Watching me watching you: How observational learning affects self-disclosure on social network sites? *Journal of Computer-Mediated Communication*, *23*(1), 34-68.

Barghuthi, N. B. A., & Said, H. (2013). Social networks IM forensics: Encryption analysis. *Journal of Communications*, *8*(11), 708-715.

Barth, S., & De Jong, M. D. T. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R., & Tang, Q. (2010). Literature overview- Privacy in online social networks. *Centre for Telematics and Information Technology, University of Twente*.

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). *T*he socialbot network: When bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference,* 93-102.

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340-347.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian, 17*, 22. http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24-31.

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook. *Information Systems Research*, *27*(4), 848-879.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on *Facebook*: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, *27*(6), 714-731.

Costa, V., & Monteiro, S. (2016). Key knowledge management processes for innovation: A systematic literature review. *VINE Journal of Information and Knowledge Management Systems, 46*(3), 386-410.

Crossler, R. E., & Bélanger, F. (2019). Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge-belief gap. *Information Systems Research*, *30*(3), 995-1006.

Cutillo, L. A., Molva, R., & Strufe, T. (2009). Privacy preserving social networking through decentralization. In *2009 Sixth International Conference on Wireless On-Demand Network Systems and Services,* 145-152. IEEE.

Deliri, S., & Albanese, M. (2015). Security and Privacy Issues in Social Networks. In *Data Management in Pervasive Systems*, 195-209. Springer International Publishing.

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

Dong, C., Jin, H., & Knijnenburg, B. P. (2015). Predicting privacy behavior on online social networks*.* In *Proceedings of the International AAAI Conference on Web and Social Media, 9*(1), 91-100.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, CO*, 339.

Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. (2015). Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, *14*(4), 447-460.

Fiesler, C., & Bruckman, A. S. (2014). Remixers' understandings of fair use online. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing,* 1023-1032.

Fink, A. (2010). *Conducting Research Literature Reviews: From the Internet to Paper*. SAGE Publications Inc.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys Tutorials*, *16*(4), 2019-2036.

Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: The privacy paradox revisited. In *International Symposium on Quantum Interaction*, 148-159, 7620. Springer Berlin Heidelberg.

Fletcher, K. P., & Peters, L. D. (1997). Trust and direct marketing environments: A consumer perspective. *Journal of Marketing Management*, *13*(6), 523-539.

Franchi, E., Poggi, A., & Tomaiuolo, M. (2015). Information and password attacks on social networks: An argument for cryptography. *Journal of Information Technology Research*, *8*(1), 25-42.

Hidayanto, A. N., Mukhodim, W. M., Kom, F. M., & Junus, K. M. (2013). A study of service quality and important features of property websites in Indonesia. *Pacific Asia Journal of the Association for Information Systems, 5*(3), 1-24.

Hossain, A. A., & Zhang, W. (2015). Privacy and security concern of online social networks from user perspective. In *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)*, 246-253. IEEE.

Houghton, D. J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services*, *28*(1-2), 74-94.

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security,* 1-15.

Kansal, P. (2014). Online privacy concerns and consumer reactions: Insights for future strategies. *Journal of Indian Business Research*, *6*(3), 190-212.

Kayes, I., & Lamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, *3-4*, 1-21.

DOI: 10.17705/1pais.14401

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In *EBSE Technical Report*, Software Engineering Group, School of Computer Science and Mathematics, Keele University, Department of Computer Science, University of Durham.

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, *69*, 29-42.

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

Krishnamurthy, B., & Wills, C. E. (2010). Privacy leakage in mobile online social networks. In *Proceedings of the 3rd Conference on Online Social Networks.*

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM Workshop on Online Social Networks,* 7-12.

Kshetri, N. (2011). Privacy and security aspects of social media: Institutional and technological environment. *Pacific Asia Journal of the Association for Information Systems*, *3*(4), 1-20.

Ladan, M. I. (2015). Social Networks: Privacy Issues and Precautions. *Proceedings of the Ninth International Conference on Digital Society*, 64-69.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159-174.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J., … & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *PLOS Medicine*, 6(7), 1-28.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: User expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference - IMC '11*, 61-70.

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

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5-12.

Matt, C., Becker, M., Kolbeck, A., & Hess, T. (2019). Continuously healthy, continuously used? -A thematic analysis of user perceptions on consumer health wearables. *Pacific Asia Journal of the Association for Information Systems, 11*(1), 108-132.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29.

Mitchell, D., & El-Gayar, O. F. (2020). The effect of privacy policies on information sharing behavior on social networks: A systematic literature review. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.*

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100-126.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior*, *26*(3), 406-418.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

Oomen, I., & Leenes, R. (2008). Privacy Risk Perceptions and Privacy Protection Strategies. *Policies and Research in Identity Management*, 261,121-138. Springer US.

Oxman, A. D., & Guyatt, G. H. (1993). The science of reviewing research. *Annals of the New York Academy of Sciences*, *703*(1), 125-134.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*(4), 977-988.

Perrin, A. (2018). Americans are changing their relationship with Facebook. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Prakash, A. V., & Das, S. (2020). Intelligent conversational agents in mental healthcare services: A thematic analysis of user perceptions. *Pacific Asia Journal of Association for Information System, 12*(2), 1-34.

Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*, *71*(9), 1089-1102.

Raine, L. (2018). Americans' complicated feelings about social media in an era of privacy concerns. *Pew Research Center.* https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339-362.

Salehan, M., Mousavizadeh, Kashipaz, S. M., & Xu, C. (2013). Information sharing on social networking websites: Antecedents and consequences of trust. In *Proceedings of the Nineteenth Americas Conference on Information Systems.*

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, *55*, 992-1000.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction 22*,111-119.

Stutzman, F., & Hartzog, W. (2012). Boundary regulation in social media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work,* 769-778.

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability*, *11*(12), 3311.

Tankovka, H. (2021a). Facebook: Number of monthly active users worldwide. *Statista*. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Tankovka, H. (2021b). Number of global social network users 2017 - 2025. *Statista.* https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Thomas, K., Li, F., Grier, C., & Paxson, V. (2014). Consequences of connectivity: Characterizing account hijacking on Twitter. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 489-500.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268.

Tufekci, C. (2007). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20-36.

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 1679-1703.

Wang, M., Liu, D., Zhu, L., Xu, Y., & Wang, F. (2016). LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing*, *98*(7), 685-708.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531-542.

Wang, Y., & Nepali, R. K. (2015). Privacy impact assessment for online social networks. In *Proceedings of the 2015 International Conference on Collaboration Technologies and Systems (CTS)*, 370-375.

Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. In *Proceedings of the International Conference on Trust and Trustworthy Computing*, 146-153. Berlin, Heidelberg.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). " I regretted the minute I pressed share" a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security,* 1-16.

Wu, Y., & Pan, L. (2021). SG-PAC: A stochastic game approach to generate personal privacy paradox access-control policies in social networks. *Computers & Security*, *102*, 102157.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, *13*(2), 151-168.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 40*(1), 38-51.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479-500.

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the General Data Protection Regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems, 12*(1), 86-122.

Appendix.

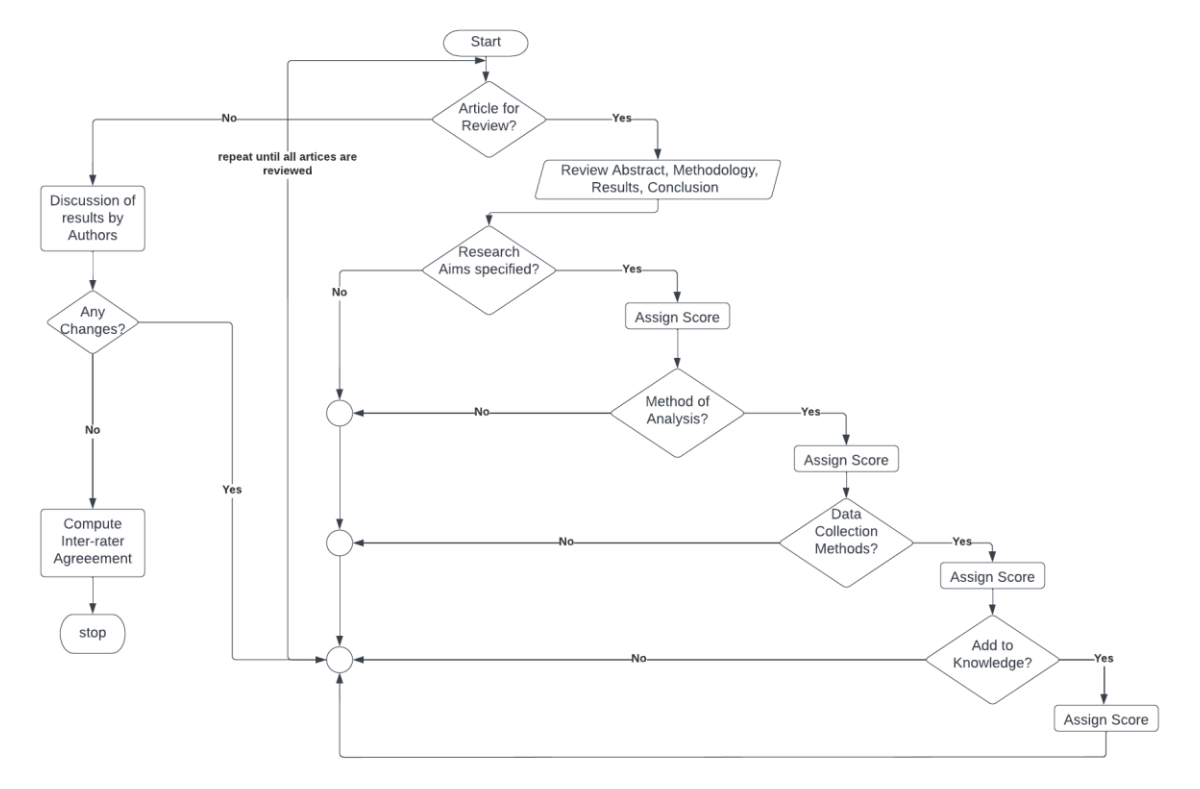

Figure 7 - Flowchart Outlining the Steps Used for the Quality Assessment of Articles

Example Paper #1

Dong, C., Jin, H., & Knijnenburg, B. P. (2015). Predicting privacy behavior on online social networks. In *Ninth International AAAI Conference on Web and Social Media*, 91-100.

In this paper an in-depth review of the abstract, introduction, methodology, results, and conclusion was performed.

In response to Quality Assessment Checklist item #1, both authors were satisfied that the research aims were clearly stated, thus a score of 1 was assigned. For example, it was stated that *"In this paper, we intend to more comprehensively study the important psychological and contextual factors that affect privacy decision making on OSN and build a cohesive privacy decision-making prediction model that can be used to assist user to make appropriate privacy decisions."*

The methodology section was then perused to find out if the paper satisfied Quality Assessment Checklist #2, both authors were satisfied that the method of analysis were appropriate and adequately explicated, thus a score of 1 was assigned. For example, it was stated that *"we present a unified framework to analyze and utilize the psychological and contextual antecedents of users' sharing decisions systematically and interactively. To do this, we provide behavioral analogs of the sharing tendency of the user, the trustworthiness of the requester/audience, the sensitivity of the information, the appropriateness of the request/disclosure, as well as several traditional contextual factors that are important antecedents of users' privacy decision making."*

The data collection section was then perused to find out if the paper satisfied Quality Assessment Checklist #3, where both authors were satisfied that the data collection

DOI: 10.17705/1pais.14401

methodologies were sufficiently detailed, thus a score of 1 was assigned. Several data collection methods were outlined in the paper, to include the use of Google+ Datasets to Location Sharing Preference Survey.

Finally, for this paper, both authors checked to see if this paper added to knowledge and understanding of the research focus under consideration. Both authors assigned a score of 1, as it was felt that the findings from this study expanded our understanding of sensitivity and self-representation in OSNs, along with the privacy decision-making prediction model that combined both psychological and contextual factors.

Table 4 - Quality Assessment Scores for Both Authors

Author	Year	Q1	Q2	Q3	Q4	Total	%
Dong et al	2015	1	1	1	1	4	100.0%

Example Paper #2

Krishnamurthy, B., & Wills, C. (2010). On the leakage of personally identifiable information via online social networks. *Computer Communication Review, 40*, 112-117.

The same processes outlined in Figure 1 were followed, and the authors both agreed that the research aims were clearly specified, and a score of 1 was assigned, as this article sought to show that it is possible for third parties to link Personal Identifiable Information (PII) and combine it with other information as “leakage”. In moving to the next assessment, both authors agreed and assigned 1, that the method of analysis was appropriate. However, the data collection methodologies could have been better articulated, and both authors assigned 0.5 which represents “Partially”, For example, it was only stated that *“For the study, we log into each OSN and perform actions, such as accessing the user profile, that cause the OSN identifier to be displayed as part of the URI. We also click on displayed ads. While performing these actions we turn on the “Live HTTP Headers” [14] browser extension in Firefox, which displays HTTP request/response headers for all object retrievals.”* We believed that more details could be given. In terms of Quality Assessment #4, we agreed that while the findings were appropriate for the study, we believed that it partially added to our knowledge and understanding, and a score of 0.5 was assigned. The final Quality Score for this paper was 3.0, which still ended in “*Good”* category.

Table 5 - Quality Assessment Scores for Both Authors

Author	Year	Q1	Q2	Q3	Q4	Total	%
Krishnamurthy et al.	2010	1	1	0.5	0.5	3	75.0%

Concept Map Creation

CASE 1

In reviewing the articles, certain themes or concepts emerged, for example in (Krishnamurthy & Wills, 2010) the common thread of concern or finding revolved around data leakage, which was highlighted in at least two other papers, and thus constituted one of the privacy concerns of OSN users. In examining the papers, different ways in which data leakage may occur were presented and it was revealed that a major area of concern is information leakage through third party applications. As such the relationship as shown on the concept map in Figure 4, highlights **Data Leakage via Third-Party Applications**, which provided a more comprehensive representation of that concern. Furthermore, Nosko et al. (2010) was one of the papers which highlighted the privacy concern of the Disclosure of Sensitive Information. However, in reviewing the papers a relationship was seen where the **Disclosure of Sensitive Information** can happen *through* **Data Leakage** and at the same time *by* **Third-Party Applications**. As such these relationships were represented on the concept map.

CASE 2

In developing the concept map for RQ #3, What are the OSN privacy policies related issues presented in the literature? It was presented in papers such as (Salehan, Mousavizadeh, & Xu, 2013) that OSN users are very concerned about the information placed in these policies and outside of not always reading the documents, users are unaware of several things. As such a part of the concept map in Figure 6 summarized what the users believe should be part of any OSN policy document. For example, the studies showed that users at times were not aware of what information is **private** or **controlled**, and it was compounded by the fact that they were not always aware of what **information** was being *shared* with **others, third-party apps,** or **OSN providers.**

https://aisel.aisnet.org/pajais/vol14/iss4/1
DOI: 10.17705/1pais.14401

About the Author

Mr. Damion Mitchell is a Ph.D. Candidate in Information Systems at the Dakota State University, specializing in Information Assurance and Computer Security. He is also affiliated with the Northern Caribbean University in Jamaica, where he serves as an Assistant Professor and Chair of the Department of Computer & Information Sciences. He holds a M.S. in Computer Science from the University of Illinois - Urbana Champaign, USA. His research interests relate to security and privacy in IoT devices, social media networks, healthcare wearables, and software engineering. He is a member of the Association of Computing Machinery (ACM).

Dr. Omar El-Gayar is a Professor of Information Systems at Dakota State University. He has an extensive administrative experience at the college and university levels as the Dean for the College of Information Technology, United Arab Emirates University (UAEU) and the Founding Dean of Graduate Studies and Research, Dakota State University. His research interests include: analytics, business intelligence, and decision support with applications in problem domain areas such as healthcare, environmental management, and security planning and management. His inter-disciplinary educational background and training is in information technology, computer science, economics, and operations research. His industry experience includes working as an analyst, modeler, and programmer. His numerous publications appear in various information technology related fields. He serves as a peer and program evaluator for accrediting agencies such as the Higher Learning Commission and ABET, as a panelist for the National Science Foundation, and as a peer-reviewer for numerous journals and conferences. He is a member of a number of professional organizations such as the Association for Information Systems (AIS) and the Association for Computing Machinery (ACM).

Copyright © 2022 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints, or via email from publications@aisnet.org.