World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:5, 2021

Users' Information Disclosure Determinants in Social Networking Sites: A Systematic Literature Review

Wajdan Al Malwi, Karen Renaud, Lewis Mackenzie

Abstract**—**The privacy paradox describes a phenomenon whereby there is no connection between stated privacy concerns and privacy behaviours. We need to understand the underlying reasons for this paradox if we are to help users to preserve their privacy more effectively. In particular, the Social Networking System (SNS) domain offers a rich area of investigation due to the risks of unwise information disclosure decisions. Our study thus aims to untangle the complicated nature and underlying mechanisms of online privacy-related decisions in SNSs. In this paper, we report on the findings of a Systematic Literature Review (SLR) that revealed a number of factors that are likely to influence online privacy decisions. Our deductive analysis approach was informed by Communicative Privacy Management (CPM) theory. We uncovered a lack of clarity around privacy attitudes and their link to behaviours, which makes it challenging to design privacy-protecting SNS platforms and to craft legislation to ensure that users' privacy is preserved.

Keywords**—**Privacy paradox, self-disclosure, privacy attitude, privacy behaviour, social networking sites.

I. Introduction

SNSs encourage their users to share quantities of personal data. Moreover, the diffusion of the smartphones throughout society, as well as the ubiquity of a variety of Internet-enabled services, has exacerbated this sharing. Besides the undoubted benefits provided by these platforms, major privacy and safety concerns have emerged worldwide, especially in the Social Networking domain.

The PEW Research Center reports on a growing number of SNS users (from 5% in 2005 to 72% in 2019). Millions of people around the world use SNSs as part of their daily routine. The reason behind this international popularity is the incredible convenience offered by these networks in allowing users to stay in touch, establish relationships and create social capital [1]. The explosive growth of SNSs has driven many scholars to pose questions regarding disclosure of private personal information as a kind of *quid-pro-quo* [2]-[7].

We carried out a SLR to synthesize research in this area. Building on the approach proposed by [8], our study delivers a set of key factors that influence users' information disclosure decisions when using SNSs. Our findings contribute to understanding the complicated nature of online privacy-related decisions.

W. Al Malwi and L. Mackenzie are with School of Computing Science, University of Glasgow, G12 8RZ, Glasgow, UK. (e-mail: w.al-malwi.1@research.gla.ac.uk, lewis.mackenzie@glasgow.ac.uk).

K. Renaud is with the University of Strathclyde, Glasgow, UK, Abertay University, Dundee, UK, and Rhodes University, South Africa (e-mail: karen.renaud@strath.ac.uk).

II. Online Privacy in SNSs

SNSs are a distinctive online social environment, where personal information provided voluntarily by users and then collected, processed and analysed [9]. Such information can be easily imported, copied, saved and distributed with others. A range of privacy violation practices have emerged as online information collection has ramped up over recent years.

The disclosure of personal information on SNS platforms has received considerable critical attention from researchers. While SNS platforms deliver undeniable benefits, the aligned privacy concerns have been keenly debated. A phenomenon identified as the *privacy paradox* has emerged: labelling the seemingly paradoxical difference between users' privacy-related behaviours and their self-reported high levels of privacy concerns.

The term privacy paradox was initially coined by Barnes [3]. It is called paradoxical because, in this case, those who claim that they value their privacy do not deploy the expected privacy protection strategies that such concerns would seem to indicate [10], [11]. The research suggests that SNS users do indeed engage in information privacy management and are not "*passive users*" as formerly referenced [12]. This means they are making deliberate trade-offs, and also that their stated privacy concerns are not as influential as anticipated in this context.

In prior studies addressing the privacy paradox phenomenon, sharing personal information on SNSs is seen as *information self-disclosure* occurring during social platform enabled connections between individuals [70], [13]. Personal information, feelings and thoughts are exchanged in most communication, reinforcing social ties [70]. This also occurs in the context of SNSs when users share private personal information with can be consumed by multiple users [14].

Individuals share their personal information for many reasons. They might want to construct social capital, enhance self-presentation, engage in impression management, and for entertainment purposes [15]. Basically, the information disclosure practices are aligned to the specific benefits offered by SNSs [16]. Because benefits will differ from person to person, such self-disclosure practices differ in scope, degree of intimacy, precision, purpose and awareness [70], [71]. CPM theory suggests that self-disclosure is typically a product of the cost/benefit evaluation process [13].

The privacy paradox phenomenon has enjoyed a great deal of attention in the research literature, with conflicting findings. A number of studies confirm the existence of the paradox e.g., [2], [3], [17]. Other studies challenge its existence e.g., [6], [7], [12] Such conflicting findings suggest that the paradox,

how it manifests and the factors that trigger it, are not yet well understood.

III. Methodology

A SLR is a high-level survey of a range of published studies on a specific topic. The SLR systematically identifies, assesses and investigates all related research evidence in order to answer a pre-defined research question or questions [8]. The main characteristic of a SLR is that it starts by developing a review protocol that defines the research grounds to systematically perform the review. There should be a clear set of objectives with pre-defined inclusion criteria for the studies. These characteristics make the SLR different than the regular literature review. SLRs aim to summarise and synthesise research results that might improve the level of validity. They also can be performed to recognise gaps and any areas that needs further investigation. Furthermore, a SLR is carried out to create a framework for new research activities [8]. In our SLR, we utilised the approach proposed by [8] to reach the intended goal. Kitchenham's methodology [8] involves seven main stages. Fig. 1 depicts the review process.

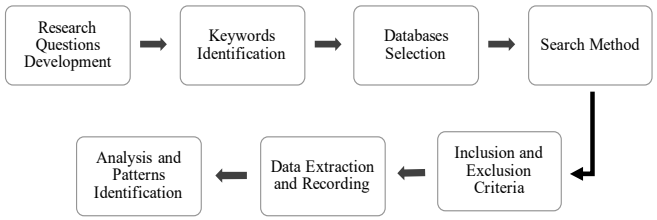

Fig. 1 SLR Process

A. Research Questions Development

A list of research questions was developed based on our original survey of SNSs privacy paradox literature, which are:

- *RQ1:* What key factors have been reported in privacy studies to determine users' information disclosure decisions on SNSs?
- *RQ2:* What platforms have been selected for investigations?
- *RQ3:* What are the participants' geographic distribution in the relevant studies?
- *RQ4:* What are the research methods adopted by researchers in the relevant studies?

B. Keyword Identification

Keywords used for the current SLR were specifically selected based on their frequency in the related literature. The selected keywords are a combination of terms including: *"self-disclosure", "privacy concerns", "privacy paradox", "privacy behaviour", "privacy attitude" and "social network sites"*. Table I shows the search queries details.

C. Databases Selection

The search process was carried out on electronic databases, including Web of Science, SCOPUS, ACM, IEEE, Science Direct and Google Scholar.

TABLE I
Search Queries and Total Counts of Relevant Papers

Search Queries	Total	Search Results	Relevant Papers
"self-disclosure" and "privacy paradox" and "social network sites"	1220	1195	25
"privacy concerns" and "self-disclosure" and "social network sites"	2930	2898	32
"privacy behaviour" and "social network sites"	341	338	3
"privacy attitude" and "privacy behaviour" and "social network sites"	58	56	2
Total Relevant Papers		62	

D. Inclusion and Exclusion Criteria

To be included, the selected studies must focus primarily on information disclosure behaviour in SNSs. Moreover, our search was restricted to papers published in English between 2003 and 2020. The reason we limit our search with this time range, is that SNSs started gaining popularity worldwide in 2003 [1].

E. Search Method

A saturation sampling approach has been implemented to ensure a comprehensive exploration. As for every search query (SQ), we extracted and recorded related papers manually. Then, when new factors were detected, they were recorded, and combined with the growing list of factors. For each SQ, we had begun with a preliminary sample including 50 search results (SR), since this sample size was a controllable starting point. Next, all the retrieved papers were reviewed, evaluated, explored, and categorised based on the inclusion criteria, yielding a set of related papers (RP). Then, the other studies were examined in rounds, where each round contains five studies (with a 10% increase of the initial round). The exploration process terminated once we have two rounds of non-relevant papers. Table II demonstrates the applied saturation sampling approach.

TABLE II
Saturation Sampling Process Details

Rounds	*SQ1*		*SQ2*		*SQ3*		*SQ4*	
	SRs	RPs	SRs	RPs	SRs	RPs	SRs	RPs
First	50	17	50	23	50	2	50	2
Second	5	1	5	2	5	1	5	0
Third	5	2	5	2	5	0	5	0
Forth	5	0	5	1	5	0		
Fifth	5	2	5	2				
Sixth	5	1	5	0				
Seventh	5	1	5	1				
Eighth	5	0	5	1				
Ninth	5	0	5	0				
Tenth			5	0				
Unique Relevant Papers		*25*		*32*		*3*		*2*

F. Data Extraction and Recording

For each relevant paper, the following information was documented including author(s), year of publication, journal and theoretical background. Each study was classified based on the used methods, population of the research participants and the selected social networking platforms. In addition, for

each paper, the research model constructs and dimensions were recorded. The original SLR results yields a large set of factors that impact information disclosure in SNSs directly and indirectly.

G. Analysis and Patterns Identification

An extensive analysis was performed to discover patterns of the retrieved factors, in order to identify specific themes. Our deductive analysis approach was guided by CPM theory developed by [13]. It maps out how private information is managed in the trade off process to balance the need of disclosure and privacy protection. Basically, our analysis stemmed from the *Cost-Benefit Calculation* or *Privacy Calculus* as an essential privacy decision criterion defined by *CPM*.

IV. Findings

This section outlines the results of the relevant papers' analysis and presents answers to the pre-defined research questions.

RQ1) What Key Factors Have Been Reported in Prior Privacy Studies to Determine Users' Information Disclosure Decisions on SNSs?

Our review identified 17 factors that play an essential role in users' privacy decision making on SNSs. These factors may impact users' information disclosure directly or indirectly. Having identified the reported factors, we further categorised them into seven key factors, as outlined in Fig. 2 and Table III in the appendix section.

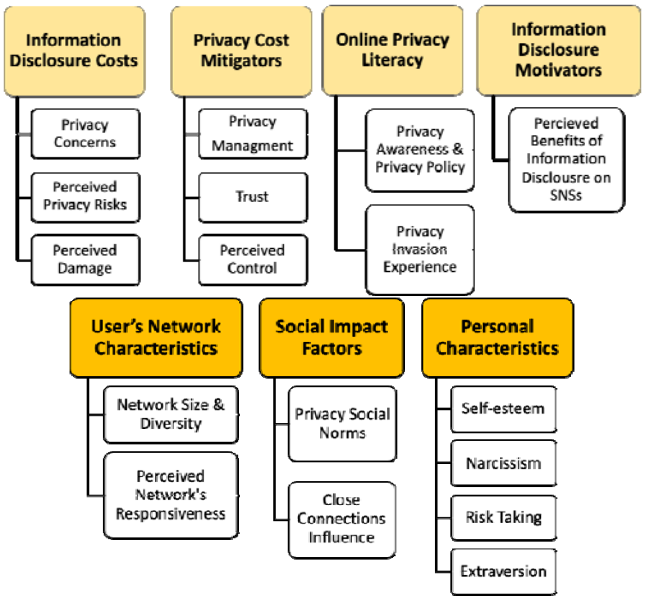

Fig. 2 Classification of the Retrieved Factors

A. Information Disclosure Costs

Information disclosure costs are inhibitors. This includes perceived privacy-related issues which negatively impact individual's decision to disclose personal information on SNSs. Since SNSs are designed as public platforms, sharing personal information on such platforms should have remarkable privacy costs. Our analysis reveals that there are three main disclosure costs: *(1) privacy concerns* e.g. [18]-[20], *(2) perceived privacy risks* e.g., [21]-[23] and *(3) perceived damage* [11], [24], [25].

A.1 Privacy Concerns: this indicates the extent to which SNS users value their privacy. This factor refers to an individual's concerns about the privacy issues associated with information disclosure. In most studies, this construct represents the cost element in the privacy calculus process. It has been frequently utilised as a predictor of self-disclosure. Specifically, once users decide to disclose private information, they are concerned about information misuse by a) SNS providers and their partners (institutional privacy concerns), and b) other platform users (social privacy concerns). Therefore, privacy can be categorised into two dimensions: (1) social and (2) institutional privacy concerns.

A.2 Perceived Privacy Risks: this relates to users' perceptions of the privacy threats related to information disclosure. It is another factor that may discourage users from sharing information on SNSs. Several studies found an evidence that users with high privacy risk perceptions reduce their information discourse [5], [26], [27].

A.3 Perceived Damage: this factor describes users' assessment of the level of damage that may occur in the event of privacy violations. Very few studies found evidence that perceived damage could lead to a user refraining from sharing their information [11], [24], [25].

B. Privacy Cost Mitigators

Our analysis uncovered several factors that might play a key role in the online privacy decision-making process, in terms of privacy cost mitigation. Three main factors emerge as privacy cost mitigators, which are: *(1) privacy management* e.g., [10], [28], [29], *(2) trust* e.g., [26], [30], [31] and *(3) perceived control* e.g., [11], [25].

B.1 Privacy Management: this term refers to the actions and strategies applied by SNS users to regulate and manage their online privacy. It has been empirically proven that SNS users employ different tactics to protect their privacy and mitigate their privacy concern, while keep disclosing information to balance between the associated costs and benefits of SNSs. There are several privacy protection strategies reported in the related studies, such as: *(1) updating the default privacy settings, (2) audience segmentation, (3) posts deletion, (4) unwanted user blocking, (5) messages encoding, (6) information falsification* and *(7) using multiple profiles with nicknames.*

B.2 Trust: the role of trust has become one of the key instruments in the related privacy studies. Trust acts as an essential determinant of privacy-related decisions. Since information disclosure behaviour embraces a certain degree of risk, trust acts as a mitigator and reduces risk perceptions. Two dimensions of trust have been identified, which are: *(1) trust in institutions (institutional trust)*, and *(2) trust in individuals (social trust)*. Accordingly, users' privacy risk perceptions will be mitigated by trust in the SNS providers

(institutional trust) *and* trust in other platform members (social trust).

B.3 Perceived Control: this factor indicates the extent to which SNS users feel that their released information is under their control. Perception of control over information is considered as privacy cost mitigator, as the high control perception will lead to more relaxed privacy concerns. On most of SNSs, certain measure of information control is offered to the public. However, users might still have concerns about the final control.

C. Online Privacy Literacy

Online privacy literacy is among the most important factors that impact SNS users' privacy behaviours. Several studies claim that paradoxical behaviour may be justified by users' lack of privacy literacy. Our analysis classifies online privacy literacy into two main constructs: *(1) privacy awareness* and the impact of *privacy policy*. e.g., [10], [32] and *(2) privacy invasion experience* e.g., [29], [33].

C.1 Privacy Awareness and Privacy Policy: privacy awareness is a key determinant that reflects the level of users' understanding and knowledge about privacy practices and violations in SNSs. It is a core factor that is tightly linked to information disclosure and privacy related decisions in SNSs, as it defines the grounds of users' perception of privacy regulation in SNSs. In addition, the presence of the platform privacy policy gives the users the impression that their information is confidential. However, [10] measures users' consumption of privacy policy and have suggested that thorough reading of the privacy policy provided by Facebook negatively impacted users' disclosure.

C.2 Privacy Invasion Experience: this factor highlights that users who have experienced privacy violation incidents, have an advanced level of online privacy literacy. Specifically, they will be more knowledgeable on how to assess privacy risks and adopt more privacy regulation strategies.

D. Information Self-Disclosure Motivators

Among others, the perceived benefits of using SNSs appear to be a significant facilitating factor. Building on the *CPM* theory, SNS users assess both benefits and costs when disclosing personal information. It has been found that information disclosure occurs when perceived benefits outweigh possible costs. Interestingly, SNS users' information disclosure depends on each individual's specific goals. In fact, findings indicate that social motivations increase the use of SNSs and correspondingly increase sharing more sensitive data. Likewise, self-presentation plays a central role in SNSs participation as users can post photos, achievements, and show their list of friends. Overall, there are some perceived benefits that motivate information disclosure in SNSs, such as:

- Relationship initiating;
- Relation maintenance;
- Social rewards: social capital, social validation, social control;
- Self-presentation;
- Enjoyment and entertainment;
- Convivence.

E. Social Impact Factors

This term has been used to describe the socially related factors, which refer to how other individuals (whether community or close connections) might influence users' privacy behaviours in SNSs. We have identified *(1) privacy social norms* and *(2) close connection influence* (peers, family) as two dimensions.

D.1 Privacy Social Norms: this factor incorporates how community members might influence user's perceptions about information privacy value. Users vary in the level of privacy valuation and their privacy social norms play a part in that aspect. For instance, users draw privacy lines depending on their perception of what others are expecting.

D.2 Close Connections Influence: this construct refers to the impact of close peers or family members privacy behaviour on the privacy decision making process. In other words, individuals tend to coordinate their privacy behaviours to be compatible with their close connections (peers, family members). Interestingly, it has been empirically proven that SNS users are more likely to adjust their profiles status into private, if their peers have already done so.

F. User's Network Characteristics

A few studies have attempted to integrate the concept of privacy decision-making in SNSs with individuals' network characteristics [31], [33], [43], [53]. That is, network characteristics have found to be impacting the level of information disclosure in SNSs. We identified *network size* and diversity and the *perceived network's responsiveness* as sub factors.

F.1 Network Size and Diversity: the increase of the network size is correlated with a higher amount of information disclosure. Likewise, there is a greater chance that individuals reveal personal information on Facebook when they have a larger list of followers in their networks [4]. However, there is an interaction between users' network diversity and information disclosure intimacy. Thus, users adjust their privacy regulation depending on their network categories (friends, family members, work colleagues).

F.2 Perceived Network's Responsiveness: a link has been found between online communication frequency and information disclosure in the context of SNSs. These platforms provide individuals with an interactive venue for receiving peer comments and feedback. Specifically, users tend to engage in an intensive information disclosure in order to receive more social rewards. Therefore, the process of information disclosure is strengthened by the number of responses and impressions received from other network members.

G. Personal Characteristics

A few personal psychological characteristics have been detected in the related studies as antecedents of information disclosure. *Narcissism, extraversion, risk taking*, and *self-esteem* were linked positively to information disclosure and shown to boost information disclosure intentions in SNSs.

RQ2: What Platforms Have Been Selected for Investigations?

The findings obtained from our SLR showed that Facebook was mainly the most investigated platform in the relevant studies with (43 RPs) followed by SNSs in general (14 papers) as demonstrated in Fig. 3, which also shows other platforms examined by the RPs. Remarkably, some of the relevant studies considered two platforms in their exploration, for instance [34].

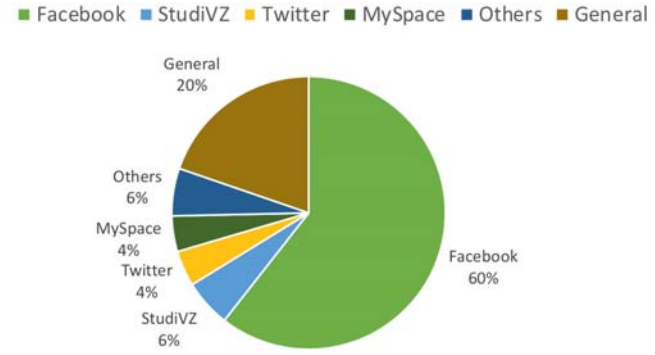

Fig. 3 Platforms Used by Relevant Papers

RQ3: What Are the Participants' Geographic Distribution in the Relevant Studies?

Our analysis indicates that the majority of the relevant papers have studied USA users' privacy behaviour intensively. Privacy paradox research in our SLR was carried out by researchers in 15 countries with USA dominating (28 RPs) followed by Europe, most were from Germany (11 RPs), then China (6 RPs). We also observed that some of the examined studies take the perspective of cross-country, such as [35] and [36]. These findings suggest that a deeper understanding of different international samples is needed in privacy paradox research, as well as a richer insight into privacy concerns from other populations other than the United States. Fig. 4 depicts the participants' geographic distribution in the included papers.

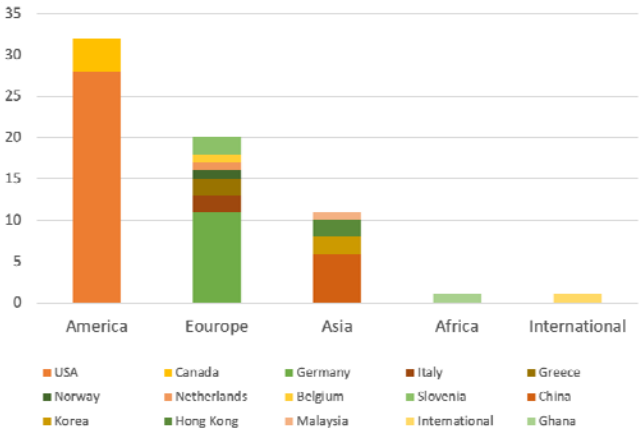

Fig. 4 Participants' Geographic Distribution

RQ4: What Are the Research Methods Adopted by Researchers in the Relevant Studies?

A wide range of methods were used to investigate the privacy paradox phenomenon. Most of the relevant studies adopted questionnaires as a primary method. Additionally, mixed methods were adopted to collect data, basically questionaries along with another method. However, a few studies used interviews to understand users' privacy perceptions. In summary, the majority of the studies (83.87%) adopted quantitative research approaches, with a few using a qualitative research approach (5%), and mixed methods (9.6%). Fig. 5 illustrates the used research methods in the RPs.

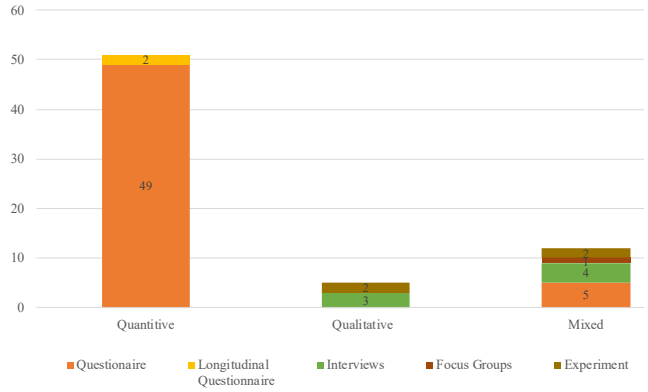

Fig. 5 The Used Research Methods in the Relevant Papers

V. Discussion

The present SLR aimed to summarise the online privacy decision-making process adopted by SNSs users through a wide set of factors. Our analysis identifies seven main determinants of information disclosure behaviour in SNSs, which are: *(1) information disclosure costs, (2) motivators, (3) privacy costs mitigators, (4) online privacy literacy, (5) user's network characteristics, (6) social impact factors and (7) personal characteristics.* It is important to highlight that prior studies might have overlooked particular privacy costs and discarded other important determinants in the context of SNSs. More specifically, the relationship between privacy concerns and information disclosure in SNSs has been thoroughly investigated. However, majority of studies have mainly emphasised privacy concerns stemming from mistrust in institutions and neglected the privacy concerns triggered by concerns about other users (social privacy concerns). Social privacy concerns have not received as much attention, with only a few studies attempting to take the first step [6], [7], [37]. Krasnova et al. [37] found that SNSs users were more concerned about social threats and their information disclosure was accordingly impacted. However, institutional privacy concerns did not affect their disclosure practices. This might help to explain the observed behavioural discrepancies discovered on some studies, which has been attributed to the privacy paradox.

The results suggest that SNSs users employ different strategies to protect their privacy and mitigate their privacy

concern, while keep disclosing enough information to balance between the associated costs and benefits of SNSs [4]. There is evidence that the available privacy settings did not address SNS privacy concerns. Accordingly, users have established further strategies to regulate their privacy such as: falsification of information, messages encoding, using multiple profiles. This has important implications for SNS providers and policy makers. We argue that understanding how privacy management impacts both privacy concerns and self-disclosure practices can provide new insights to privacy policies makers and SNS providers to help them to design systems that effectively reflect the privacy needs of SNS users.

Our analysis goes beyond previous reports, showing that most research on the privacy paradox phenomenon was conducted in USA specifically. There have been a few empirical investigations that conducted a cross-country perspective, and these often examine the variances between the US and another country. Since the original SNSs rise was in the United States, perhaps it was not unexpected that most prior research have investigated users' behaviours in America followed by Europe. However, given that SNSs have become popular worldwide, there is a crucial need for more information privacy studies to shed the light on multiple countries while non-student samples are preferable. Thus, a deeper understanding of different international samples is needed as well as a richer insight into privacy concerns from other populations other than the United States.

The findings demonstrate that Facebook has been identified as a dominant platform, and this was confirmed. There might be a need to examine users' online privacy practices on a broader set of platforms to understand whether users' behaviour might change in response to the platform's affordances and standards.

VI. Conclusion and Future Work

The SLR provides a comprehensive overview of research into the privacy paradox phenomenon in SNSs. We cast a light on information disclosure determinants that have been observed in the online privacy behaviour literature. Altogether, we were able to summarise the key factors that predict information disclosure in SNSs in order to highlight research gaps. Such findings contribute to understanding the complicated nature of online privacy-related decisions in SNSs. It supports the design of privacy-protecting systems and tools, as well as formulation of privacy policies that accommodate users' privacy concerns. Furthermore, such a study will deliver important insights to SNSs providers by identifying key determinants of users' information disclosure behaviour. Such providers could then create designated instruments to resolve the defined privacy issues and thus ensure platform sustainability. The current SLR could be further employed as a framework for new studies. In our future work, based on the frequency of the retrieved factors, a set of core determinants has been detected. A comprehensive research model has been created incorporating all the identified factors. The model will be validated via a triangulation study, implementing an explanatory sequential design procedure where each phase builds on the results of the previous phase.

Appendix

TABLE III
Details of the Retrieved Factors

Factors		Citation	#
Information Self-Disclosure Costs	Privacy Concerns: Institutional Privacy Concerns Social Privacy Concerns.	[4]-[7], [10], [11], [18]-[20], [24], [25], [29], [34], [35], [38]-[53]	30
	Perceived Privacy Risks	[5], [7], [15], [21]-[23], [26], [27], [36], [41], [44], [50], [54], [55]	14
	Perceived Damage	[11], [24], [25]	3
Privacy Costs Mitigators	Privacy Management	[4], [5], [10], [17], [22], [27]-[30], [34], [35], [42], [45], [47], [48], [53], [56]-[61]	22
	Trust: Trust in Providers Trust in SNSs Members	[11], [18], [21], [24], [26]-[28], [30], [31], [39], [40], [43], [48], [49], [51], [54], [55], [58], [59], [62]	21
	Perceived Control	[7], [11], [15], [24], [25], [39], [49], [50], [54], [55], [62]	11
Online Privacy Literacy	Privacy Awareness	[18], [25], [27], [41], [47], [54], [63]	7
	Privacy Policy	[10], [18], [23], [50]	4
	Privacy Invasion Experience	[23], [29], [33], [41], [65]	5
	Privacy self-efficiency	[19], [35]	2
Information Self-Disclosure Motivators	Information Self-Disclosure Perceived Benefits	[5], [7], [11], [19], [20], [22], [26], [30], [31], [35], [36], [46], [52], [57], [59], [60], [65]-[68]	19
Social Impact Factors	Privacy Social Norms	[18], [53]	2
	Social Influence	[29], [59], [62]	3
User's Network Characteristics	Network Size and Diversity	[4], [23], [34], [58] [47]	4
	Perceived Network's Responsiveness	[69]	1
Personal Characteristics	Self-Esteem	[31]	1
	Risk Taking	[43]	1
	Extraversion	[33]	1
	Narcissism	[53]	1

References

[1] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship," *J. Comput. Commun.*, vol. 13, no. 1, pp. 210-30. 2007.

[2] R. Gross, A. Acquisti, and H. J. Heinz, "Information revelation and privacy in online social networks," in WPES'05: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 71-80. 2005.

[3] S. B. Barnes, "A privacy paradox: Social networking in the United States", vol. 11, no. 9, 4 September, *First Monday*, 2006.

[4] A. L. Young and A. Quan-Haase, "Information revelation and internet privacy concerns on social network sites," *Proceedings of the Fourth International Conference on Communities and Technologies*, pp. 265, 2009.

[5] F. Xu, K. Michael, and X. Chen, "Factors affecting privacy disclosure on social network sites: An integrated model," *Electron. Commer. Res*., vol. 13, no. 2, pp. 151–168, 2013.

[6] A. Gruzd and Á. Hernández-García, "Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media," Cyberpsychology, *Behav. Soc. Netw*., vol. 21, no. 7, pp. 418–428, 2018.

[7] M. Jozani, E. Ayaburi, M. Ko, and K. K. R. Choo, "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," *Comput. Human Behav.,* vol. 107, no. January, p. 106260, 2020.

[8] B. Kitchenham, "Procedures for performing systematic reviews," Keele Univ. Natl. ICT Aust., 2004.

[9] Govani and Pashley, "Student Awareness of the Privacy Implications When Using Facebook," *Educ. Law*, vol. 9, pp. 1-17, 2005.

[10] F. Stutzman, R. Capra, and J. Thompson, "Factors mediating disclosure in social network sites," *Comput. Human Behav*., vol. 27, no. 1, pp. 590–598, Jan. 2011.

[11] H. Krasnova and N. F. Veltri, "Privacy calculus on social networking sites: Explorative evidence from Germany and USA," *Proc. Annu. Hawaii Int. Conf. Syst. Sci*., pp. 1–10, 2010.

[12] A. L. Young and A. Quan-Haase, "Privacy Protection Strategies on Facebook: The Internet privacy paradox revisited," *Inf. Commun. Soc*., vol. 16, no. 4, pp. 479–500, 2013.

[13] S. Petronio, "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples," *Commun. Theory*, vol. 1, no. 4, 1991.

[14] C. Y. Lai and H. L. Yang, "Determinants of individuals' self-disclosure and instant information sharing behavior in micro-blogging," *New Media Soc*., vol. 17, no. 9, pp. 1454-1472, 2015.

[15] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: why we disclose," J. *Inf. Technol.,* vol. 25, pp. 109–125, 2010.

[16] J. L. Gibbs, N. B. Ellison, and R. D. Heino, "Self-Presentation in Online Personals," *Communic. Res.,* vol. 33, no. 2, pp. 152-177, 2006.

[17] Z. Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bull. Sci. Technol. Soc*., vol. 28, no. 1, pp. 20-36, 2008.

[18] L. N. Zlatolas, T. Welzer, M. Heričko, and M. Hölbl, "Privacy antecedents for SNS self-disclosure: The case of Facebook," *Comput. Human Behav.,* vol. 45, pp. 158–167, Apr. 2015.

[19] T. Dienlin and M. J. Metzger, "An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample," *Journal of Computer-Mediated Communication*, vol. 21, no. 5, pp. 368-383, 2016.

[20] J. Min and B. Kim, "How are people enticed to disclose personal information despite privacy concerns in social network sites? the calculus between benefit and cost," *Journal of the Association for Information Science and Technology*, vol. 66, no. 4, pp. 839-857, 2015.

[21] Z. Liu and X. Wang, "How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison," *Inf. Manag.,* vol. 55, no. 8, pp. 1005–1023, Dec. 2018.

[22] H. Lee, H. Park, and J. Kim, "Why do people share their context information on social network services? a qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk," *Int. J. Hum. Comput. Stud*., vol. 71, no. 9, pp. 862–877, 2013.

[23] K. Li, L. Cheng, and C. I. Teng, "Voluntary sharing and mandatory provision: Private information disclosure on social networking sites," *Inf. Process. Manag*., vol. 57, no. 1, p. 102128, Jan. 2020.

[24] B. Contena, Y. Loscalzo, and S. Taddei, "Surfing on Social Network Sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes," *Comput. Human Behav*., vol. 49, pp. 30–37, Aug. 2015.

[25] T. Alashoor, S. Han, and R. C. Joseph, "Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model," *Commun. Assoc. Inf. Syst*., vol. 41, no. August, pp. 62–96, 2017.

[26] C. W. Chang and J. Heo, "Visiting theories that predict college students' self-disclosure on Facebook," *Comput. Human Behav*., vol. 30, pp. 79–86, Jan. 2014.

[27] L. N. Zlatolas, T. Welzer, M. Hölbl, M. Heričko, and A. K. Kamišalíc, "A Model of Perception of Privacy, Trust, and Self-Disclosure on Online Social Networks." *Entropy*, vol. 21, no. 8, pp. 772.

[28] P. K. Masur and M. Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies," *Soc. Media Soc.,* vol. 2, no. 1, 2016.

[29] Z. Jingzhi, W. Weiquan, K. Lara, and K. Sung, "Actual privacy self-disclosure on online social network sites: Reflective-impulsive model," 26th Eur. Conf. Inf. Syst. Beyond Digit. - Facet. Socio-Technical Chang. *ECIS*, 2018.

[30] M. J. K. Choon, "Revisiting the privacy paradox on social media: An analysis of privacy practices associated with Facebook and Twitter," *Can. J. Commun*., vol. 43, no. 2, 2018.

[31] 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?," *Cyberpsychol. Behav*., vol. 12, no. 3, pp. 341-345, 2009.

[32] H. Xu, T. Dinev, H. Jeff Smith, P. Hart, and H. Jeff, "Examining the Formation of Individual' s Privacy Concerns: Toward an Integrative View, *ICIS*, 2008.

[33] M. Koohikamali, D. A. Peak, and V. R. Prybutok, "Beyond self-disclosure: Disclosure of information about others in social network sites," *Comput. Human Behav*., vol. 69, pp. 29–42, Apr. 2017.

[34] Y. H. Choi and N. N. Bazarova, "Self-Disclosure Characteristics and Motivations in Social Media: Extending the Functional Model to Multiple Social Network Sites," *Hum. Commun. Res.*,vol. 41, no. 4, pp. 480-500, 2015.

[35] H. T. Chen, "Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management," *Am. Behav. Sci*., vol. 62, no. 10, pp. 1392-1412, 2018.

[36] Z. Liu, X. Wang, and J. Liu, "How digital natives make their self-disclosure decisions: a cross-cultural comparison," *Inf. Technol*. People, vol. 33, no. 2, pp. 5380-558, 2019.

[37] H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva, "Privacy concerns and identity in online social networks," *Identity Inf. Soc.,* vol. 2, no. 1, pp. 39–63, 2009.

[38] H. Krasnova, E. Kolesnikova, and O. Günther, "'It won't happen to me!': Self-disclosure in online social networks," 15th Am. Conf. Inf. Syst. 2009, *AMCIS*, vol. 4, pp. 2559–2567, 2009.

[39] S. Taddei and B. Contena, "Privacy, trust and control: Which relationships with online self-disclosure?," *Comput. Human Behav*., vol. 29, no. 3, pp. 821–826, May 2013.

[40] H. Krasnova, N. F. Veltri, and O. Günther, "2132xSelf-disclosure and privacy calculus on social networking sites: The role of culture intercultural dynamics of privacy calculus," *Bus. Inf. Syst. Eng*., vol. 4, no. 3, pp. 127–135, 2012.

[41] G. Oppong et al., "Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective." *Behavioral Sciences*, vol. 8, no. 6, pp. 58.

[42] A. Heravi, S. Mubarak, and K. K. Raymond Choo, "Information privacy in online social networks: Uses and gratification perspective," *Comput. Human Behav*., vol. 84, pp. 441–459, Jul. 2018.

[43] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Human Behav.,* vol. 25, no. 1, pp. 153–160, Jan. 2009.

[44] M. Tsay-Vogel, J. Shanahan, and N. Signorielli, "Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviours among Facebook users," *New Media Soc*., vol. 20, no. 1, pp. 141-161, 2018.

[45] F. Stutzman, J. Vitak, N. B. Ellison, R. Gray, and C. Lampe, "Privacy in interaction: Exploring disclosure and social capital in Facebook," in *Proceedings of the 6th International AAAI Conference on Weblogs and Social Media*, 2012.

[46] E. Tzortzaki, A. Kitsiou, M. Sideri, and S. Gritzalis, "Self-disclosure, Privacy concerns and Social Capital benefits interaction in FB: A case study," in *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, pp. 1-6, 2016.

[47] 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-Disclosure1," *J. Comput. Commun*., vol. 19, no. 2, pp. 248–273, 2014.

[48] C. Shane-Simpson, A. Manago, N. Gaggi, and K. Gillespie-Lynch, "Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital," *Comput. Human Behav*., vol. 86, pp. 276–288, Sep. 2018.

[49] B. Davazdahemami, A. Luse, B. Hammer, and P. Kalgotra, "The role of parallelism in resolving the privacy paradox of information disclosure in social networks," in *International Conference on Information Systems, ICIS*, 2018.

[50] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view," *Int. Conf. Inf. Syst. Proc*., 2008.
[51] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in Association for Information Systems - *13th Americas Conference on Information Systems, AMCIS*: *Reaching New Heights,* 2007.
[52] A. Kitsiou, E. Tzortzaki, M. Sideri, and S. Gritzalis, "Digital privacy and social capital on social network sites. friends or foes?," in *6th Workshop on Socio-Technical Aspects in Security and Trust*, 2016.
[53] S. Utz and N. C. Kramer, "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms," *J. Psychosoc. Res. Cybersp*., vol. 3, no. 2, 2009.
[54] T. Kroll and S. Stieglitz, "Digital nudging and privacy: improving decisions about self-disclosure in social networks" *Behav. Inf. Technol*., vol 40., no. 1, pp. 1-19, 2019.
[55] Z. Liu, X. Wang, Q. Min, and W. Li, "The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model," *Inf. Syst. J.,* vol. 29, no. 2, pp. 279-316, 2019.
[56] H. T. Chen and W. Chen, "Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection," *Cyberpsychology, Behav. Soc. Netw*., vol. 18, no. 1, pp. 13-19, 2015.
[57] A. Chennamaneni and A. Taneja, "Communication privacy management and self-disclosure on social media - A case of Facebook," 2015 *Am. Conf. Inf. Syst. AMCIS*, pp. 1–11, 2015.
[58] W. Xie and C. Kang, "See you, see me: Teenagers' self-disclosure and regret of posting on social network site," *Comput. Human Behav.,* vol. 52, pp. 398–407, Jun. 2015.
[59] M. Walrave, I. Vanwesenbeeck, and W. Heirman, "Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults," *Cyberpsychology*, vol., 6, no. 1, 2012.
[60] P. Li, H. Cho, and Z. H. Goh, "Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus," *Telemat. Informatics*, vol. 41, pp. 114–125, Aug. 2019.
[61] E. L. Spottswood and J. T. Hancock, "Should I Share That? Prompting Social Norms That Influence Privacy Behaviors on a Social Networking Site," *J. Comput. Commun*., vol. 22, no. 2, pp. 55-70, 2017.
[62] C. Christy, L. Z. W. Y., and C. T. K. H., "Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence," *Internet Res.,* vol. 25, no. 2, pp. 279–299, Jan. 2015.
[63] F. Youssouf Osman and N. Z. A. Rahim, "Self-disclosure and Social network sites users' awareness," *Int. Conf. Res. Innov. Inf. Syst. ICRIIS'11*, 2011.
[64] M. Bartsch and T. Dienlin, "Control your Facebook: An analysis of online privacy literacy," *Comput. Human Behav*., vol. 56, pp. 147–154, Mar. 2016.
[65] P. B. Brandtzæg, M. Lüders, and J. H. Skjetne, "Too many facebook 'Friends'? Content sharing and sociability versus the need for privacy in social network sites," *Int. J. Hum. Comput. Interact*., vol. 26, no. 11-12, pp. 1006-1030, 2010.
[66] S. Trepte and L. Reinecke, "The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study," *Comput. Human Behav*., vol. 29, no. 3, pp. 1102–1112, May 2013.
[67] C. Hallam and G. Zanella, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards," *Comput. Human Behav*., vol. 68, pp. 217–227, Mar. 2017.
[68] 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," *J. Commun*., vol. 64, no. 4, pp. 635–657, 2014.
[69] R. M. Walsh, A. L. Forest, and E. Orehek, "Self-disclosure on social media: The role of perceived network responsiveness," Comput. Human Behav., vol. 104, p. 106162, Mar. 2020.
[70] Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self disclosure. *Human Communication Research*, vol. 2, no. 4, pp. 338-346. doi:10.1111/j.14682958.1976.tb00494.
[71] Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*, Holt, Rinehart & Winston.