“Who should I grant access to my post?”: Identifying the most Suitable Privacy Decisions on OSNs

ARTICLE INFO

Keywords:
Online Social Networks
Privacy Calculus
Audience Types
Information Sensitivity
Self-disclosure

ABSTRACT

Purpose – Online social networks (OSNs) provide users with mechanisms such as social circles and individual selection to define the audiences (i.e., privacy policy) of the shared information. This privacy decision-making process is a hard and tedious task for users because they have to assess the cost-benefit in a complex environment. Moreover, little is known about how users assess the cost-benefit of matching the elements of online communication and their interests. Therefore, the purpose of this paper is to develop and test a research model to understand the impact that the types of receivers and the sensitivity of messages have on privacy decisions.

Design/methodology/approach – A study was conducted to understand how users evaluate the cost-benefit of the disclosure action in online social networks for the different types of receivers identified and the sensitivity of the message. Data from 400 respondents was collected and analyzed using partial least squares modeling.

Findings – The findings of this study demonstrated a trade-off variance between the perceived cost-benefit and the disclosure of sensitive information with different receiver types. Disclosing personal information with trusted receivers, influencer receivers, and receivers from the circle of coworkers had a positive significant effect on social capital building. Conversely, disclosing personal information with receivers from the circle of family or unknown receivers had a significant negative effect on social capital building and even a significant positive effect on privacy concerns.

Originality/value – Recent literature has documented the increasing interest of the research community in understanding users’ concerns and interests in making the most suitable privacy decisions. However, most researchers have worked on understanding the disclosure action from a user-centered perspective and have not considered all of the elements of online communication. This study puts the focus on all of the elements of communication during disclosure actions, taking into account the properties of the message and receivers and the impact on users’ cost-benefit value.

1. Introduction

As social network users, we are constantly faced with decisions that are the product of interaction and socialization with others that have a direct impact on our privacy. Research studies have shown that when we are faced with these decisions in online communication, we always assess the cost-benefit of the decision (Quah and Haldane, 2007). This process is well-known as the *Privacy Calculus theory*[1]. However, the privacy concept is very complex, and the number of factors to assess in online communication is higher than in traditional communication (e.g., the number of friends, the relationship types, the persistence of the information, etc.). Moreover, these decisions have tremendous importance because they may negatively affect our privacy and reputation (Wang et al., 2011). Because of this, we often have difficulty in assessing the cost-benefit of disclosure decisions, which leads us to regret our decisions. In order to avoid regrets, decisions need to be made with information that is as perfect as possible, even though research experiments have demonstrated that we seldom have perfect information for deciding (Acquisti et al., 2015).

Research on online communication and users’ behavior has studied a wide range of factors and relationships to explain information disclosure decisions in OSNs (Quan-Haase and Young, 2010; Park et al., 2009; Liu and Brown, 2014). Most of these factors are related to the user transmitting the information through the following: personal characteristics, such as personality traits, gender, motivation for using the social network (self-presentation, enjoyment, building relationships, etc.); network usage characteristics, such as time of use, the number of friends, and the number of interactions with other users; and users’ perceptions about information control, subjective norms, benefits, risks, etc. However, factors that are external to the transmitter (e.g., the sensitivity of the information, confidence in the channel, types of receivers, etc.) have been less studied. The study of communication elements study has been in

ORCID(s):

[1] Privacy Calculus theory states that individuals always rationally weigh the potential benefits and potential risks of data disclosure decisions.

decreasing order, the transmitter, the channel, the message, and, ultimately, the receiver. In traditional communication, the combination of the factors of the elements of communication favors effective communication similarly, the factors of the elements (channel, message, and receiver) in online communication must also be considered in order to favor communication that is free of regrets. The main objective of these studies is to understand the self-disclosure action of the users and which factors favor it and which do not. They do not, however, analyze in detail which factors are considered by a user for granting or denying access to a specific contact for a post (i.e., fine-grained privacy decisions). Thus, there is a gap in explaining which factors of communication elements and their combinations produce benefits and which produce privacy risks. Finally, although self-disclosure decisions may have a negative impact on our privacy, several studies state that when people share their thoughts, feelings, or information with others would gain a psychological benefit to themselves (Esterling et al., 1999; Gable et al., 2004) that may improve the individual's physical and mental health (Niederhoffer and Pennebaker, 2009). Therefore, we can consider social well-being as a positive effect of self-disclosure.

The main objective of this work is to understand the privacy decision-making process in social networks by making sense of each decision choice of the communication elements. We analyze the impact of communication elements factors on privacy risks and social benefits in order to make suitable privacy decisions and how these finally contribute to the users' social well-being. To do this, we have developed a research model for individually granting/denying receivers access to information published in OSNs. We test our research model with real users to obtain feedback about how these factors influence the privacy decision-making process. The resulting model could be used to improve current privacy mechanisms, automatizing the assessment of the cost-benefit trade-off for each potential receiver, leading to suitable privacy policy decisions and to the improvement of the social well-being of users.

The paper is organized as follows. Section 2 includes a literature review about the social benefits and privacy for the disclosure process in OSNs. Section 3 presents our research model and the relevant factors regarding communication elements. Section 4 describes the research methodology. Section 5 presents the results obtained. Section 6 discusses the main findings. Finally, Section 7 presents some concluding remarks and future work.

2. Literature review

2.1. Privacy calculus theory and privacy decisions

The assessment of social benefits and privacy cost (well-known as Privacy Calculus theory) is a complex task that users should complete for effective communication in social networks (Bennet and Bennet, 2008). This theoretical privacy calculus framework has been proven in the OSN domain by a large number of research works (Krasnova et al., 2010; Schiffrin et al., 2010; Chen and Shen, 2015; Kim and Kim, 2018; Guo et al., 2020). For example, Guo et al. (2020) analyze help-request campaigns in online social networks where users face the dilemma of helping friends and losing privacy or not helping friends and preserving their privacy. Their results indicated that privacy assurance and relationship closeness jointly influenced recipients' privacy concerns and social rewards influenced participation behaviors. However, these research works have mostly assessed the users' perceptions and preferences towards the privacy risks and social benefits of information disclosure in a general way. When users face an OSN privacy decision, this decision has several sub-decisions that are directly linked to the elements of the communication. A clear example is when a user is going to share his/her holiday experience, he/she has to choose a social network on which to share it (the channel). The user then creates the publication (the message), and finally selects the social circles or audience that will have access to it (the receivers). This is when the receivers generate positive or negative responses (the feedback), which is related to social benefit building and loss of privacy (and possibly bad reputation), respectively. Therefore, there is a gap in the individual factors of those sub-decisions that may contribute or stand in the way of disclosing a specific message with a specific receiver.

Furthermore, privacy calculus is a short-term assessment that users make before making decisions. Literature reviews in human behavior show that online social well-being is usually tested as a long-term assessment of users' satisfaction for all decisions made (Huang, 2016). The online social well-being of users can be seen as the individual's consciousness and feelings about their whole social lives, which consists of perceptions of pleasure, positive emotions, and greater satisfaction. Previous studies have tested well-being with respect to users' benefits (Huang, 2016; Ko and Kuo, 2009); however, very little research has been done to test social well-being with respect to users' privacy cost.

The research model proposed in this study analyzes which factors of the communication elements involved in privacy sub-decisions and to what extent they contribute to the privacy calculus theory. In addition, the long-term impact of these sub-decisions is tested by studying the social well-being of users.

2.2. Information disclosure and benefit

Disclosure actions can be defined as communicating personal information to other people (Derlega and Chaikin, 1977). The degree of disclosure is often based on trust and tries to reinforce the closeness of people. In OSNs, information disclosure actions can be carried out either using texts (status updates, commenting, location sharing, or private messages) or through other non-verbal means (sharing photos, videos, or links). Users generally tend to disclose different forms and types of information in order to achieve different gratifications. For instance, maintaining social relationships, seeking attention, feedback, and communications are some of the major gratifications that users seek by self-disclosing in OSNs (Quan-Haase and Young, 2010; Park et al., 2009). Furthermore, unlike traditional communication, in online communication (social networks), disclosure actions require the selection and configuration of more elements than just the message. It also involves the choice of the channel and the receivers, which in traditional communication is inherent by the context.

Tidwell and Walther (2002) found that people tend to disclose more information in OSNs compared to traditional communication. In addition, according to Nguyen et al. (2012), the information disclosed is more sensitive. Some researchers such as Vitak and Ellison (2013) defend the ease of sharing information as a cause, while others relate this to the maintenance of users' contacts with weak ties. Another factor that they consider is the number of Facebook friends a user has. This could influence the user's self-disclosure since many of the social connections on Facebook require a certain degree of self-disclosure. Moreover, it has been shown that trust in contacts and in the social network platform influences the self-disclosure of information by users, which increases it (Taddei and Contena, 2013). These studies test the factors that influence the users' self-disclosure, but not how these factors provide them benefit. Other studies on the social benefit of self-disclosure, such as Ko and Kuo (2009) and Liu and Brown (2014), have been done. However, those studies did not analyze the benefit obtained by information disclosure with certain factors of communication elements, with the exception of the study by Huang (2016) where several dimensions of self-disclosure (that included sensitive information) were tested. By extending the factors with respect to the channel, the message, and the receiver, the understanding of users' perceived benefit and efficient online communication could be advanced.

Focusing on the benefits of disclosing information, previous studies have used several theories to measure benefits such as social capital theory (Ko and Kuo, 2009; Liu and Brown, 2014; Church et al., 2017), social support (Chen and Shen, 2015; Huang, 2016), motivation-based theory (Krasnova et al., 2010; Koohikamali et al., 2019), and other less popular theories such as Xu et al. (2013). However, these theories have not been sufficiently supported by the community of behavioral science studies, except for social capital theory. Therefore, we apply the well-known social capital theory to online communication to investigate the motivations behind users' behaviors of self-disclosure. Social capital is a theoretical framework that considers the benefits that individuals accrue from interactions with members of their social network (Bourdieu, 1985). For instance, Choi et al. (2018) analyze the privacy risks and expected social capital gains in social connectivity management by examining the key types of social information that users consider and their behavioral responses to online friend requests. This work concludes that social information network mutuality (i.e., friends in common) and profile analysis are considered in evaluating privacy risks and expected social capital gains. They also state that the likelihood of no-action and the likelihood of accepting friend requests is influenced by the expected social capital gains and privacy risk evaluation. Social capital is typically divided into two categories: bonding social capital and bridging social capital. Bonding social capital consists of the physical, emotional, and social support that an individual can provide to another member within the network. It is often associated with homogeneous dense networks and close intimate relationships since they are more likely to provide emotional aid and companionship than acquaintances (Wellman and Wortley, 1990). Choi et al. (2015) analyze how information dissemination and network commonality influence the perceived privacy invasion and relationship bonding, and therefore, influence individuals' behavioral responses. Bridging social capital consists of information resources and influence among members of heterogeneous networks. According to Granovetter (1977), this kind of social capital is more likely among users with "weak ties" because they can provide more novel information and new perspectives than close relationships. Usually, bridging social capital provides the benefit of feeling connected to a larger group and having contact with a broad range of people. In OSNs environment, users can assess the social capital for both categories by taking into account the closeness of the relationship that supports them (bonding social capital), and the number of people reached (bridging social capital) (Vitak and Ellison, 2013).

In the study, we analyze specifically how the factors of the communication elements involved in privacy subdecisions contribute to building social capital (specifically bonding and bridging social capital) for users. In particular, factors such as trust, scope, and control of the information besides the sensitivity of the message and the different types of receivers are considered in this study.

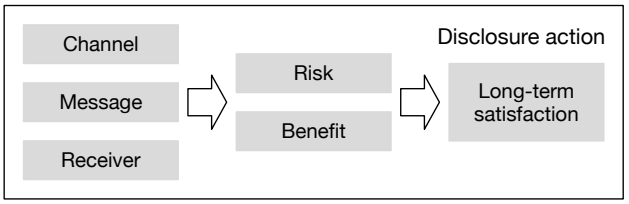

Figure 1: Conceptual model.

2.3. Privacy cost and overexposure

The flip side of disclosing information on social networks is the loss of privacy and the potential consequences of it. In the literature, a rich discussion of the nature, definition, and conceptualization of privacy is offered. As Hallam and Zanella (2017) claim, privacy can be defined as a right, a commodity, and a state. This representation of privacy as a commodity matches the privacy calculus theory where users' privacy (the cost) is exchanged for social rewards (the benefits).

To measure the cost in privacy decisions, prior research used perceived privacy risks and/or privacy concerns to reflect the cost dimension of the privacy calculus equation. For instance, to measure the cost of self-disclosure decisions, Hallam and Zanella (2017) defined information privacy in four taxonomic dimensions: collection, unauthorized secondary use, improper access, and errors. Conversely, Kim and Kim (2018) consider that risk appraisal emerges from the vulnerability and the severity perceived in OSN decisions. These privacy concerns generally reflect a personal predisposition to worry about privacy and are therefore antecedent to risk beliefs, which are defined as the expectation of losses related to self-disclosure (Krasnova et al., 2010). For the purpose of our study, we measure the privacy risk through users' privacy concerns about their information privacy on a website.

Similar to the research on perceived benefits by disclosure actions, most research focuses on the influence of factors on self-disclosure (e.g., Vitak and Ellison (2013); Liu and Brown (2014)) and on understanding how perceived cost influences self-disclosure (e.g., Krasnova et al. (2010); Hallam and Zanella (2017)). For this reason, very little is understood about how different kinds of factors related to communication impact users' cost during self-disclosure decisions. A few researchers have tested the users' cost perception of sharing sensitive information (Xu et al., 2013) and of sharing different types of personal information (Kim and Kim, 2018), but no one has tested factors related to the receiver.

Finally, we analyze in this study how the factors of the communication elements involved in privacy sub-decisions represent a privacy cost for users by considering their privacy concerns. In this way, the study will shed light on the action of relinquishing to users' privacy in exchange for social rewards.

3. Research model and hypothesis development

The research model of this study is designed to explain the impact of the element properties of online communication (channel, message, and receiver) on users' assessment of social capital building and privacy concerns during information disclosure. In addition, it also includes the assessment of those perceptions (benefit and cost) regarding the users' final online social well-being, which can be interpreted as a long-term assessment of the benefits-costs of disclosure actions. All of the factors considered in our study are framed as dimensions of the disclosure action. Figure 1 provides the conceptual model used for the current study. Figure 2 presents the developed research model after the development of the hypotheses.

3.1. Channel factors

In online communications, the users' decision regarding the channel may be done at the OSN environment level (i.e., choosing the social network), or it may be done in a social network level (i.e., choosing the disclosure mechanism such as stories, wall-publications, or direct messages). The channel choice sheds light on the way users choose their preference for disclosing information on one social network platform and not on another; the mechanism choice sheds light on the properties that the disclosing mechanism offers to users. In this study, we focus on the properties of the privacy decision-making process of the channel from the first approach (the social network choice). Therefore, we assess how users' perceptions either support or do not support the users' privacy calculus evaluation. To do this, we

consider two well-known factors: trust in the OSN provider, and the users' perceived capacity to control their actions.

3.1.1. Trust in the OSN provider

In previous literature, researchers describe trust as a multidimensional factor with different meanings. Some researchers consider *trust as a belief*, which may produce benefits, while other researchers interpret *trust as an intention*, which is linked to assuming risks (Krasnova et al., 2010). In our work, we assess trust in both senses as a belief and intention in the reliability, truth, or ability of the OSN provider to link it with both sides of the privacy calculus (benefit vs. cost). Most of the time, trust in providers has positive impacts (e.g., on the willingness to participate in transactions in E-commerce (Kim et al., 2008; Ponte et al., 2015) and on self-disclosure in social networks (Sun et al., 2015)). When users have a high level of trust in providers their interactions are generally enhanced, helping them to open up and seek help from other members of the community (increasing their bonding social capital) and generating interactions on an ongoing basis such as valuable advice and new information sources (increasing their bridging social capital) (Chen and Shen, 2015). Hence, based on this reasoning, trust in the OSN provider may positively empower the users' perceived benefits regarding disclosure actions, increasing their bonding and bridging social capital. However, with the new social network reports and scandals about the usage of user data (Isaak and Hanna, 2018), we want to confirm that trust in the OSN provider is still a cost-mitigating factor and contributes to social capital building. Therefore, we hypothesize the following:

H1. *Users' trust in the OSN provider is negatively related to their perceived privacy risk.*

H2. *Users' trust in the OSN provider is positively related to the building of (a) bonding social capital and (b) bridging social capital.*

3.1.2. Perceived Control

Perceived control over information refers to the capacity that people have to control information released online. Factors that determine the perception that people have of information control are related to how websites collect, store, and utilize users' personal information. Social networks offer users different privacy mechanisms and privacy settings to control the scope of their information. Some mechanisms provide more granularity, allowing users to choose the desired audience for each publication individually or based on social groups, while others use always the same social group (followers or friends). Xu et al. (2008) empirically demonstrate the importance of providing self-controlling mechanisms to impact the perception of privacy calculus on OSNs. Krasnova et al. (2010) considered perceived control as a cost-mitigating factor, and they validated this hypothesis in their study. Also, by allowing users to control their information, Lee et al. (2013) state that better choices can be made about the audience (specialized receivers). In this sense, users with high control of information dissemination mechanisms can select the contacts that have previously provided (or are expected to provide) them with more benefits. Either through greater physical, emotional or social support (increasing their bonding social capital) or through new sources of information and opportunities (increasing their bridging social capital). Hence, we hypothesize the following:

H3. *Users' perceived control is negatively related to their perceived privacy risk.*

H4. *Users' perceived control is positively related to the building of (a) bonding social capital and (b) bridging social capital.*

3.2. Sensitivity of the message

The information contained in a publication has great relevance in privacy calculus. Many works have reported regrets on social networks because of the information that users shared, mainly due to disclosing too much personal information or inappropriate information (Wang et al., 2011; Such et al., 2017; Alemany et al., 2020). In social networks, most users are identifiable so that their actions bring them social benefits (Vitak and Ellison, 2013). As a consequence, the users' data becomes personal, but how does the sensitivity value of data in disclosure actions contribute to the users' cost-benefit? Kim and Kim (2018) assessed different types of personal data and how it impacts benefits and risks in video recommendation systems. They found a significant impact on all of the personal information types regarding risk appraisal. According to the definition by Huang (2016), self-disclosure has five dimensions: amount, depth, honesty, intent, and valence. In our study, we assess self-disclosure on OSNs taking into account the sensitivity dimension that corresponds to depth, which is defined as *"the degree of intimacy of the information topic revealed"*. Oeldorf-Hirsch and Sundar (2015) observed an empowering effect on users' benefits regarding the benefit

of the information-sharing activity. Based on these pieces of evidence, we believe that *"Users' depth-disclosure action is positively related to their perceived privacy risk"* and also that *"Users' depth-disclosure action is positively related to the building of bonding social capital and bridging social capital"*. However, since users always share personal information because it is linked with their OSN profile that usually identifies them and the message decision is always made together with the receiver decision, we researched our beliefs but adapted for different types of potential receivers. As we discuss in the next section, the depth-disclosure action with different types of receivers could affect users' privacy calculus in different ways. Therefore, we reformulated them into new hypotheses by including a specific receiver in the depth-disclosure action.

3.3. Differences between types of receivers

The privacy policy choice in social networks is essentially about deciding the receiver for a specific message (the publication). In this environment, the user interacts with user types that have different properties that could affect the privacy risks and social benefits of the user. Features such as the visibility/influence of users on the network and trust in other users have been used by Squicciarini et al. (2014) and Alemany et al. (2018) to assess user risks and calculate a privacy score for specific users. Many other works such as (Yang et al., 2014) have recently used these same features to calculate privacy policy recommendations for users. The influencer user's role, which is growing in popularity on social networks, is able to enhance the visibility of the user's information while the trusted user's role can ensure more secure communication of information. In addition to these types, users interact with other types based on social circles, even with unknown users (Yang et al., 2014). The types represented by social circles often contain their own rules and information routines that can affect cost and benefit in different ways. Houghton et al. (2013) analyzed the influence of different social circles on image sharing and showed that information sharing with different types of relationships has a significant effect on the quality of the relationship. Furthermore, Wang et al. (2011) who studied the most common regrets of social network users have stressed the relationship between regrets and disclosing information with some social circles such as family, friends, and coworkers. Therefore, we analyzed the types based on the primary social circles defined by Dunbar (2010). Some of these types of receivers may overlap in a real user; however, for simplicity we consider them separately in this study. Therefore, in our research model, we analyzed the dissemination action with different types of receivers and how they compute for privacy.

3.3.1. Trusted receivers

The strength of a relationship is a (probably linear) combination of the amount of time, the emotional intensity, the intimacy (mutual confiding), and the reciprocal services that characterize the relationship (Granovetter, 1977). Previous studies in E-commerce have shown that trust toward other members can positively impact the willingness to participate, generating social benefits (Chen and Shen, 2015). Nahapiet and Ghoshal (1998) suggested that when trust exists between the parties, they are more willing to engage in reciprocal interaction by helping others with the intention of receiving help in turn. Hence, we believe that the trust towards other members may increase users' level of bonding social capital. On the other hand, Nonaka (1994) indicated that interpersonal trust is important in teams and organizations for creating an atmosphere for knowledge sharing. We believe that the trust in others may increase this knowledge sharing enhancing the bridging social capital. According to Privacy Calculus theory, trust can be seen as a way to reduce the perceived costs of disclosing information and encourage users to interact among them. Krasnova et al. (2010) have studied the relationship between trust in members (as a cost mitigating factor) and privacy risks but with no conclusive results. Therefore, we hypothesize the following:

H5-1. *Users' depth-disclosure action with trusted users is negatively related to their perceived privacy risk.*

H6-1. *Users' depth-disclosure action with trusted users is positively related to the building of (a) bonding social capital and (b) bridging social capital.*

3.3.2. Influencer receivers

The influencer role is a combination of desirable attributes (be they personal attributes like credibility, expertise, enthusiasm, or be they network-related attributes such as connectivity or centrality) that allows someone to influence (produce an effect on) others (Bakshy et al., 2011). There are many research papers that analyze the users' characteristics to influence other users (Myers et al., 2012; Cheng et al., 2014). Interacting with those users may potentially promote the visibility of a regular-user. This technique is commonly used in the design of optimal marketing strategies (Galeotti and Goyal, 2009). Social capital definition includes this aspect of border openness for obtaining social benefit by users, so, we believe that interacting with influencer users may increase the social capital of users. However,

it might turn out to be a double-edged sword when unintended audiences access personal information (Wang et al., 2011). This risk could be measurable for users (Williams, 2006). Based on this reasoning, we also believe that the interaction with influencer users can extend the users' information visibility causing potential privacy risks. Therefore, we hypothesize the following:

H5-2. *Users' depth-disclosure action with influencer users is positively related to their perceived privacy risk.*

H6-2. *Users' depth-disclosure action with influencer users is positively related to the building of (a) bonding social capital and (b) bridging social capital.*

3.3.3. Social circle-based receivers

Generally, each social circle contains its own rules and information routines. When we disclose information with one of them, depending on how sensitive the information is, it can affect users' cost and benefit in different ways. Reports of regret on social networks such as those of Wang et al. (2011) and Such et al. (2017) have provided evidence of regret by divulging too much personal information with specific social circles. Differences between the most common social circles and their properties may have a common impact on users' cost-benefit. For our study, we have analyzed four different social circles, three of which are based on a simplification of Dunbar's relationship theory (Dunbar, 2010) (friends, family, and coworkers) and a new one based on the OSN domain to represent unknown users. These social circles also match the reasons for the disclosure decisions regretted by users in (Wang et al., 2011).

The reports about regrets on social networks (Wang et al., 2011; Such et al., 2017) indicate that most of regrets were related to disclosing too much personal information with close users like friends, family, and coworkers. It seems users are more concerned about their information when receivers are in a social circle that is closer to them (family, then friends, then coworkers). In contrast, there is also concern about unknown (or distant acquaintance) users accessing personal information (Malik et al., 2016). Therefore, we hypothesize the following:

H5-3. *Users' depth-disclosure action with friends is positively related to their perceived privacy risk.*

H5-4. *Users' depth-disclosure action with family members is positively related to their perceived privacy risk.*

H5-5. *Users' depth-disclosure action with coworkers is positively related to their perceived privacy risk.*

H5-6. *Users' depth-disclosure action with unknown users is positively related to their perceived privacy risk.*

With regard to the social benefits of disclosing personal information with each of these social circles, the context of these relationships may change the perceived benefits by users. Sylaska and Edwards (2014) showed that, generally, friends and family members provide emotional support (which is related to bonding social capital) when disclosing information about personal issues, and coworkers provide informational support (which is related to bridging social capital). Also, professional networks encourage information exchange, promote interpersonal relationships, and lead to improvements in productivity and loyalty, which contributes to informational support (Kasavana et al., 2010). Thus, friends and family members have less propensity to contribute to bridging social capital, and, conversely, coworkers have less propensity to contribute to bonding social capital. For users with no relationship with the user (i.e., unknown receivers), even though the interaction may provide informational support (like the coworker social circle), by sharing intimate information with them negative reactions may be elicited for a more public social circle (Bazarova, 2012). Therefore, we expect a positive impact on social bonding by providing emotional or substantive support for friends and family circles, and we expect a negative impact on social bonding for coworkers and unknown users. In contrast, disclosing information with social circles that are not close may positively impact social bridging building. Thus, we hypothesize the following:

H6-3. *Users' depth-disclosure action with friends is (a) positively related to the building of bonding social capital and (b) negatively related to the building of bridging social capital.*

H6-4. *Users' depth-disclosure action with family members is (a) positively related to the building of bonding social capital and (b) negatively related to the building of bridging social capital.*

H6-5. *Users' depth-disclosure action with coworkers is (a) negatively related to the building of bonding social capital and (b) positively related to the building of bridging social capital.*

H6-6. *Users' depth-disclosure action with unknown users is (a) negatively related to the building of bonding social capital and (b) positively related to the building of bridging social capital.*

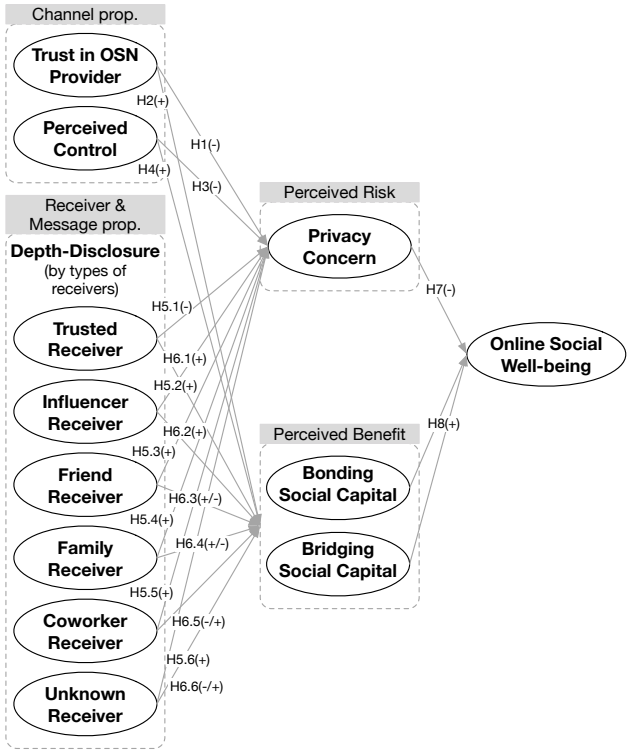

Figure 2: Research model.

3.4. Online Social Well-being

According to Niederhoffer and Pennebaker (2002), self-disclosure can improve an individual's physical and mental health from a positive psychology perspective. Moreover, it has been shown that positive reactions collected from social capital building contributes to improving the users' well-being (Schiffrin et al., 2010). In contrast, the users' concern regarding OSN risks is related to negative experiences resulting in a heightened awareness of privacy-related issues and increased privacy concerns. Those negative experiences could hinder the psychological state of users, impacting on their social well-being (Xu et al., 2012). Thus, we hypothesize the following:

H7. *Users' perceived privacy risk is negatively related to their online social well-being.*

H8. *Users' building of (a) bonding social capital and (b) bridging social capital is positively related to their online social well-being.*

The overall research model is described in Figure 2.

4. Methodology

This study presents an initial attempt to investigate the role of receivers' properties and message sensitivity in the users' assessment of potential benefits and risks of data disclosure decisions in social networks. We also investigate how messages and receivers contribute indirectly to users' online social well-being. The research setting, data collection method, measurement, and demographics of the respondents are reported below.

4.1. Research settings

For this study, we chose the users of Facebook as the main object of discussion since it is one of the most popular and widely used online social networks. Launched in February 2004, Facebook allows its users to define different kinds of connections/relationships with each other (e.g., friends, acquaintances, followers, etc.) and to create social elements (e.g., groups, posts, albums, preferences, etc.) for interacting with others in a whole variety of ways (e.g.,

comments, tags, mentions, direct messages, etc.). More importantly, unlike other online social networks, Facebook offers users many mechanisms to decide all of the elements of online communication for users' disclosing actions in a fine-grained way. Users have complete and free capability to choose the channel, message, and receivers (by selecting a specific privacy policy) in a disclosure action. Therefore, we believe Facebook users are perfect for investigating the influence of these elements on users' cost-benefit perceptions (Privacy Calculus) and on the disclosure action.

4.2. Data collection

The data used in this study were collected through a survey created on Google Forms and shared through Prolific Academy (Peer et al., 2017), which is an online participant recruitment platform for surveys and market studies. The questionnaire that was developed for the survey was pre-tested by six researchers, three of whom are experienced in surveys and quantitative research. Their remarks and suggestions were used to make improvements and to clarify some questions, which led to the final version of the questionnaire. We also made a very small-sample experiment with colleagues to avoid potential errors (such as technical blips) and to measure the average time required for completing the questionnaire. Then, we linked the questionnaire to a study in Prolific. Before publishing the study, we made a custom pre-screening of the target audience of the study using the menus of Prolific. As required features for participating in the study, we selected the following: (`r1`) fluent English language comprehension so that the questionnaire was understood completely; (`r2`) being a regular Facebook user in order to fit our target population; (`r3`) a minimum of 50 completed studies on Prolific; and (`r4`) an approval rate greater than 90% for quality control. For quality control, we also included some attention check questions in the questionnaire asking participants to select a specific answer. The participants that answered at least one attention question incorrectly were excluded from the study. Finally, we published the study, and, after the participants completed it, we managed to collect completed questionnaires from 400 participants. The resulting files (demographic data from Prolific, and the questionnaire responses from Google Forms) were collected and joined for their later analysis.

4.3. Measurement

All of the measures in this study have been used and validated in prior studies (see Appendix A). Minor changes in the wording were made in order to fit the current research context. Social bonding and social bridging were measured with items adapted from Williams (2006). Privacy concern was measured with items adapted from Xu et al. (2013). Perceived control and trust in Facebook were measured by items adapted from Krasnova et al. (2010). Online social well-being was measured by items adapted from Church et al. (2017) and Ellison et al. (2007). In addition, we took the dimension of depth (related to sensitivity of information) in information disclosure measured by items adapted from Wheeless and Grotz (1976) as a reference in order to customize them for different types of receivers. Instruments for all of the constructs were presented on a five-point Likert scale, anchored from "1 = never" and "5 = always". We used a unipolar scale because, in comparison with a bipolar scale (such as "1 = strongly disagree" and "5 = strongly agree"), it allows users to focus on a single item's absence or presence, which may generate more accurate answers[2]. For each statement, the participants were asked to indicate how often participants agreed with the statement.

4.4. Sample characteristics

The demographic statistics of the respondents are reported in Table 1. Of the 400 respondents, 45.5% of them were male and 54.5% were female. The respondents' ages ranged from 18 to 76 years old with a positive skewness distribution (0.879), which means their ages had a major concentration in younger ages (below 35.3 years, average). Approximately 75.5% of the respondents were not students, and the majority of them were employed (around 70%). In addition, the respondents were mainly from Europe (87%), North-America (8%), and Australia (3%). Among European respondents, there was a high concentration of UK respondents (47%), followed by Portuguese (9.5%), Poles (7.5%), Italians (4.2%), and Spaniards (3.2%). We split the nationalities into sub-regions following the Eurovoc thesaurus to facilitate the reading of Table 1.

5. Analysis and results

The proposed research model was tested using partial least squares (PLS) analysis using Smart PLS 3.2.9 because PLS employs a component-based approach for estimation that minimizes residual distributions (Chin, 1998) and is best suited for testing complex relationships by avoiding inadmissible solutions and factor indeterminacy (Chen et al.,

[2] https://www.questionpro.com/blog/unipolar-likert-scale/

Table 1
Demographic information (n = 400).

Measure	Items	Value (frequency)
Age	Range	18-76 years old
	Average	35.3 years old
Gender	Male:	182 (45.5%)
	Female:	218 (54.5%)
Nationality	Western EU:	216 (54.0%)
	Southern EU:	77 (19.3%)
	Central/Eastern EU:	47 (11.7%)
	Northern EU:	8 (2.0%)
	North-America:	32 (8.0%)
	Australia:	12 (3.0%)
	Others:	8 (2.0%)
Student status	Yes:	98 (24.5%)
	No:	302 (75.5%)
Employment status	Full-Time:	194 (48.5%)
	Part-Time:	80 (20.0%)
	Unemployed:	48 (12.0%)
	Other:	78 (19.5%)

2011). Moreover, PLS has less stringent sample size and indicator distribution requirements, as compared to the covariance-based structural equation modeling (SEM) approaches. Following the two-step data analytical procedures (Hair et al., 1998), the measurement model was first examined to evaluate the reliability and validity of measures, and then the structural model was tested to estimate the hypothesized relationships.

5.1. Measurement model assessment

We evaluate the measurement model by examining the convergent validity and discriminant validity of measurement items. Convergent validity can be assessed by examining the factor loadings, the composite reliability, and the average variance extracted (AVE). Specifically, composite reliability refers to the internal consistency of the indicators measuring a given factor, and average variance extracted indicates the amount of variance captured by a construct as compared to the variance caused by the measurement error. Table 2 presents some descriptive statistics, composite reliability values, Cronbach's alpha values, and the average variance extracted of the principal constructs. A composite reliability of 0.70 or above and an average variance extracted of more than 0.50 are deemed acceptable. Cronbach's alpha scores of 0.70 or greater are also considered acceptable, while scores between 0.8 and 0.9 are considered satisfactory (Fornell and Larcker, 1981). All of the values of composite reliabilities and Cronbach's alpha exceed 0.70, verifying the reliability of measurement items. From these facts, we conclude that convergent validity is fulfilled (i.e., constructs that theoretically should be related are in fact related). Appendix B extends Table 2 information including more statistic data and the factor loadings for each of the measured items.

Discriminant validity is established by initially ensuring that an indicator's outer loading on a construct is greater than cross-loadings with other constructs and the by ensuring that the square root of AVE is higher than the outer correlations for each construct (Fornell and Larcker, 1981). Table 2 also presents the correlation matrix of the constructs and the square root of the average variance extracted for each construct. The results show that all outer loadings are greater than cross-loadings for each construct and that squared root of AVEs are higher than outer correlations. The results affirm discriminant validity (i.e., constructs that are not supposed to be related are actually unrelated). Overall, the results show the high reliability and validity of the posited measurement model.

Furthermore, variance inflation factors (VIF) were used to assess the degree of multicollinearity in the measures of our study. This test assesses how much the variance of an estimated regression coefficient increases if your predictors are correlated. The VIFs ranged from 1.030 to 2.351, which are all below the suggested threshold of 3.3 (Kock, 2015). Therefore, we did not find a significant multicollinearity problem in this study.

5.2. Structural model assessment

The results of the analysis are provided in Table 3 and Figure 3. Table 3 presents the overall explanatory power with the hypotheses, the estimated path coefficients (β), and the associated t-value of the paths (all significant paths are indicated with asterisks). Figure 3 visually summarizes the results of the conceptual model with r-squared (R^2),

Table 2
Results of convergent validity and discriminant validity analyses. Squared root of Average Variance Extracted (diagonal elements in bold) and correlation between constructs (off-diagonal elements).

	Mean	SD	AVE	CR	CA	Construct											
						PC	TF	CN	BO	BR	DT	DI	DF	DA	DC	DU	SW
PC	3.69	1.14	.689	.917	.887	**.830**											
TF	2.16	1.05	.759	.904	.841	-.473	**.871**										
CN	3.04	1.08	.698	.874	.785	.318	.506	**.835**									
BO	2.83	1.28	.515	.889	.859	-.156	.299	.180	**.718**								
BR	2.86	1.15	.542	.922	.906	-.131	.353	.283	.483	**.736**							
DT	2.27	1.09	.733	.916	.877	-.111	.202	.077	.493	.353	**.856**						
DI	1.59	0.87	.667	.889	.832	-.046	.177	.038	.296	.317	.475	**.817**					
DF	2.38	1.09	.727	.914	.874	-.120	.176	.015	.336	.300	.670	.389	**.853**				
DA	2.48	1.25	.786	.936	.908	-.049	.219	.091	.265	.281	.579	.388	.636	**.887**			
DC	1.56	0.84	.777	.933	.904	-.120	.200	.056	.342	.268	.468	.558	.546	.526	**.882**		
DU	1.24	0.65	.705	.905	.840	-.021	.076	.070	.169	.234	.339	.594	.284	.206	.562	**.840**	
SW	3.07	1.01	.705	.905	.857	-.279	.435	.362	.317	.332	.175	.096	.152	.168	.187	.103	**.815**

Note: SD=standard deviation; AVE=average variance extracted; CR=composite reliability; CA=Cronbach's Alpha; PC=privacy concern; TF=trust in Facebook; CN=perceived control; BO=bonding social capital; BR=bridging social capital; DT=depth-disclosure action with trusted receivers; DI=depth-disclosure action with influencer receivers; DF=depth-disclosure action with friends; DA=depth-disclosure action with family members; DC=depth-disclosure action with coworkers; DU=depth-disclosure action with unknown users; SW=online social well-being.

path coefficients, and p-values. A test of significance of all paths was performed using the bootstrap resampling procedure. The research model of this study explains 25.1% of the variance in users' perceived privacy concern, 31.5% in users' perceived bonding social capital, and 26.6% in users' perceived bridging social capital for the intention of disclosing personal information with different types of receivers. Moreover, the model explains 19.1% of the variance in online social well-being as the product of all decisions made. In order to ensure that the findings of the analysis are not confounded by other variables, we controlled the possible effect of users' demographic information (age, gender, nationality, and student status) on perceived risk, perceived benefit, and online social well-being. All of the control variables were excluded from the final model due their insignificance. Therefore, the research model demonstrates satisfactory explanatory power to capture the effect of privacy trade-off between the different communication elements and users' self-disclosure decisions, and, in consequence, with their online social well-being.

The findings demonstrate that users' trust perception in the OSN provider (the channel), which in our case is Facebook, has great relevance in the privacy trade-off: decreasing the users' privacy concern (β = -0.417, $p < 0.001$), which supports H1; and increasing the users' perception of bonding social capital ($\beta = 0.159$, $p < 0.01$) and bridging social capital ($\beta = 0.193$, $p < 0.001$), which supports H2a and H2b. The relationships between perceived control and benefits-risks are also significant, which supports H3 (β = -0.117, $p < 0.05$) and H4b ($\beta = 0.158$, $p < 0.01$), except for bonding capital building (H4a) which was not supported.

The findings further indicated interesting results between the depth dimension of self-disclosure and the different types of receivers. For the disclosure with trusted receivers, there was a significant increasing relationship with both dimensions of social capital, which supports H6-1a ($\beta = 0.463$, $p < 0.001$) and H6-1b ($\beta = 0.229$, $p < 0.01$), while no significant relationship was found with privacy concern (H5-1). For the disclosure with influencer receivers, there was only a significant increasing relationship with bridging capital (H6-2b), while H5-2 and H6-2a were not supported. For the disclosure with friend receivers, there was not a significant relationship with privacy concern (H5-3) or with social capital (H6-3a and H6-3b). For the disclosure with family members, we found a significant increasing relationship with users' privacy concern ($\beta = 0.161$, $p < 0.01$) and a significant decreasing relationship with social capital (β = -0.145, $p < 0.05$), which supports H5-4 and H6-4a and does not support H6-4b. Finally, for the disclosure with coworkers and unknown receivers, there was only a strong relationship between coworkers and bonding social capital ($\beta = 0.209$, $p < 0.01$) and a strong relationship between unknown receivers and bonding social capital (β = -0.129, $p < 0.05$), which supports H6-5a and H6-6a, respectively. Therefore, the rest of the hypotheses that link the depth dimension of self-disclosure with receivers were not supported (H5-5, H6-5b, H5-6, and H6-6b).

Finally, as we expected, the users' perceptions of benefits and risks of self-disclosure with their online social well-

Table 3
Partial least squares path estimators for the research model.

H	Relations	β	t	Results
H1	trust in facebook → privacy risk	-.417	7.44^{***}	supported
H2a	trust in facebook → social bonding	.159	3.06^{**}	supported
H2b	trust in facebook → social bridging	.193	3.83^{***}	supported
H3	perceived control → privacy risk	-.117	2.13^{*}	supported
H4a	perceived control → bonding sc	.073	1.42	non-supported
H4b	perceived control → bridging sc	.158	2.99^{**}	supported
H5-1	DD: trusted receiver → privacy risk	-.038	0.58	non-supported
H6-1a	DD: trusted receiver → bonding sc	.463	7.12^{***}	supported
H6-1b	DD: trusted receiver → bridging sc	.229	3.29^{**}	supported
H5-2	DD: influencer receiver → privacy risk	.053	0.85	non-supported
H6-2a	DD: influencer receiver → bonding sc	.067	1.12	non-supported
H6-2b	DD: influencer receiver → bridging sc	.124	2.01^{*}	supported
H5-3	DD: friend receiver → privacy risk	-.104	1.43	non-supported
H6-3a	DD: friend receiver → bonding sc	-.014	0.19	non-supported
H6-3b	DD: friend receiver → bridging sc	.051	0.70	non-supported
H5-4	DD: family receiver → privacy risk	.161	2.48^{**}	supported
H6-4a	DD: family receiver → bonding sc	-.145	2.21^{*}	supported
H6-4b	DD: family receiver → bridging sc	.010	0.15	non-supported
H5-5	DD: coworker receiver → privacy risk	-.100	1.37	non-supported
H6-5a	DD: coworker receiver → bonding sc	.209	3.25^{**}	supported
H6-5b	DD: coworker receiver → bridging sc	-.018	0.24	non-supported
H5-6	DD: unknown receiver → privacy risk	.052	0.82	non-supported
H6-6a	DD: unknown receiver → bonding sc	-.129	2.27^{*}	supported
H6-6b	DD: unknown receiver → bridging sc	.050	0.75	non-supported
H7	privacy risk → online social well-being	-.223	5.00^{***}	supported
H8a	bonding sc → online social well-being	.177	3.58^{***}	supported
H8b	bridging sc → online social well-being	.218	3.96^{***}	supported

Note: $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

being had strong significance, which supports H7, H8a, and H8b. The relationship between privacy concern and their online social well-being had a significantly decreasing impact (β = -0.223, $p < 0.001$). The relationships between the two social capital dimensions (bonding capital ($\beta = 0.117$, $p < 0.001$) and bridging capital ($\beta = 0.218$, $p < 0.001$)) and their online social well-being had a significantly increasing impact.

6. Discussions

The current study has evaluated users' privacy trade-offs (cost-benefit) in the privacy decision-making process in social networks taking into account the different element properties of communication. The relationship between the theory of privacy calculus (PCT) and users' trade-off perceptions of the properties of the receiver, message, and channel was conceptualized and empirically tested, performing a study about the participants' online social network usage. While there was a mix of supported and unsupported hypotheses in the results, the change in significance between constructs of depth-disclosure actions by receiver types and the perceived benefit-risk was the most interesting.

There was a striking significance between the trust factors (trust in the OSN provider, and trust in other users) and the users' perceptions of benefits. As previous research works state (Kim et al., 2008; Ponte et al., 2015) and our study confirms, trust in the OSN provider helped to reduce the users' privacy concerns (H1) and increase the users' perception of both dimensions of social capital building (H2a and H2b) to the same extent. Trust in other users significantly increased both dimensions of social capital building (H6-1a and H6-1b), but there was a stronger impact on bonding capital. However, there was no relation between trust in members and privacy concerns. For the control perceived by users, there was a less significant effect than trust factors on users' perceived benefits-risks. This also helped to reduce the privacy concerns (H3) and partially increase the social capital building of users (only for the bridging capital, H4b).

When disclosing personal information to different kinds of users, there was a significant difference in users' privacy calculus perception. As we predicted, based on OSN users' regrets (Wang et al., 2011), the social circle of family

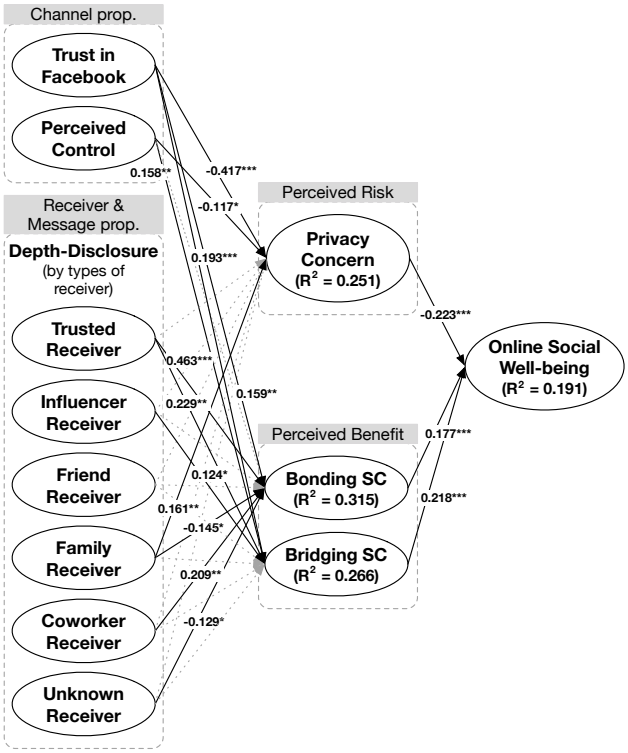

Figure 3: Results of the research model. Note: — represents a significant link, ···· represents an insignificant link, $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

members had a significantly positive impact on users' privacy concerns (H5-4) and a partially negative impact on social capital building (H6-4a). Although the social circle of coworkers also showed some limited evidence of regrets as in the family case, our study did not find a significant effect on users' privacy concerns, but we found a significant positive effect on bonding social capital (H6-5a). This behavior might be explained by a desire for strengthening ties with coworkers with whom we spend an important amount of time daily and for the seeking of job satisfaction (Huang and Liu, 2017). Curiously, the social circle of friends had no significant effect on users' perceptions of benefit or risk. It could be that the friend social circle has become the most open to interpretation for the users. For instance, social networks like Facebook collapse other context relationships within friends (Davis and Jurgenson, 2014), so this social circle blends in with a lot of other types of receivers. As we predicted, disclosing personal information with influencer receivers had a significantly positive effect on bridging capital building (H6-2b), while there was not a significant impact on users' privacy concerns. Users do not perceive disclosing their information with influencer users to be risky. However, if they do not know them (unknown receivers) and they disclose their personal information, it has been shown that there is a significantly negative effect on their bonding capital (H6-6a). Taken together, these findings reveal that relationships that are too close (family) or, the flip side, unknown relationships are perceived by users as not being beneficial. Conversely, disclosing users' personal information with highly trusted receivers and influencer receivers improves their social capital building. Generally, most of the relations between depth-disclosure with different receivers and user privacy concerns did not have a significant relationship. As Krasnova et al. (2010) state, this could be due to the fact that user privacy concerns mainly center on organizational risks such as the collection and secondary use of their information. Users may believe companies have more incentive to abuse their information compared to other network members (except for family members who are a conflicting audience). Also, many of the relations between depth-disclosure with different receivers and bridging social capital did not have a significant relationship. This could be due to the fact that not all of the members of a specific social circle contribute in the same way to this factor and that the features (trust and influence) of an individual are those that produce a significant effect on bridging social capital.

Finally, the findings confirm that the benefit and risk constructs that we tested contributed to the online social

well-being of users, inversely relating users' privacy concerns with online social well-being (H7) and directly relating social capital with online social well-being (H8a and H8b).

6.1. Theoretical implications

This study contributes to the existing literature in the following three important ways. First of all, we introduce a new approach to the privacy decision-making process on OSNs as the composition of multiple decisions related to choosing the elements of online communication (channel, message, and receiver). Previous research was mainly focused on exploring self-disclosure as a single decision. They just modeled users' perceptions of the social network properties (the channel) and users' interests, and how these constructs impacted their social benefits and privacy risks (Chen and Shen, 2015; Chang and Heo, 2014; Jiang et al., 2013). Those research works took an approach that is closer to OSN business features in order to increase the number of users' self-disclosing actions instead of an approach that focuses on users' privacy and their understanding of online communication. In contrast, the research presented in our work takes into account the users' perspective focusing on privacy decision-making. This result is in the line with protecting users and its privacy, and the continuous proposals of mechanisms (e.g., Squicciarini et al., 2014; Yang et al., 2014) to compute the most beneficial and, in turn, less risky privacy policies for disclosure decisions in OSNs.

Second, our study offers a valuable contribution to the Privacy Calculus theory (Krasnova and Veltri, 2010) by providing results about the impact of the elements of online communication on the users' perceptions of privacy risk and social benefit. It is important to note that people disclose their personal information as a continuous trade-off between relinquishing some privacy in exchange for some social benefits. Our findings confirm and extend the comprehension of this theory to the decisions about the elements of online communication. Therefore, academic attention to the depth-disclosure action with potential receiver types will generate a more comprehensive picture of information disclosure on social networks and will further improve our current understanding of which features contribute to users' benefit and risk and to what extent they contribute.

Third, this study extends the usual properties considered in the state of the art of disclosure analysis in OSNs, especially in the case of receivers (which are commonly based on trust and intimacy). These new properties are based on the different types of receivers and the social circles to which they belong. The usage of these properties was raised from the mechanisms that are commonly offered by social networks to users for privacy policy selection. Similarly to the research work by (Kim and Kim, 2018) where different types of personal information were investigated, our findings revealed differences in significance between the social circle of belonging of receivers and the privacy calculus perception. In contrast to the findings of Kim and Kim (2018) for different types of personal information, our study found more relationships between depth-disclosure actions (by types of receivers) and users' perceived benefit than between depth disclosure actions and risk perceptions. These findings could improve the understanding and prevention of users' regrets on social networks and online communication (Wang et al., 2011).

6.2. Practical implications

The current research also has several implications for practitioners in the context of social networking apps. It has been shown that privacy decisions are a burdensome task because users have too many connections (also known as friends), and they are required to assess the disclosure decision for each one. These research results shed light on the relevance of each factor in privacy decision-making and its relationship with others. A better classification of users' relationship types, trust estimation, and the visibility properties of a user on the network could provide improvements in current privacy mechanisms. Those mechanisms combined with our results could help to recommend suitable privacy policies, automatizing the individual process of privacy calculus and maximizing the users' social benefits obtained by disclosing their information. Therefore, recommending audiences that are highly trusted, influential, or belong to the social circle of coworkers will be prioritized over other audiences such as family members or unknown users that might reduce the benefit of the user or even increase his/her risk. For example, a user belonging to a social circle of coworkers with a high level of trust and influence on others will be recommended as an audience for a social network post, while family members will not be recommended (unless there is an extremely high level of trust with the user).

6.3. Limitations and future research

While the current research provides several implications for theory and practice, there are limitations that must be acknowledged and opportunities to be considered for future research. Even though the sample size of our study is sufficient, it could be unbalanced or biased for some external and uncontrollable factors. The reiterative confirmation of the presented findings should be performed to validate that our samples are not biased. In our findings, we

observed a few more significant relationships for perceived benefit than for perceived risk. According to Hallam and Zanella (2017), users easily perceive benefits as being closer, while privacy risks are perceived as being abstract and psychologically distant. Thus, a limitation of our work is that we do not know how our proposed research model could fit a population that is only composed of participants that have had negatives experiences when disclosing personal information on social networks. Another limitation was the constructs used. We mainly checked the self-disclosure decision and the influence of properties of other elements of online communication. However, individually analyzing the decisions for those elements could shed light on their suitability for users' self-disclosure. Our future research will be directed towards the application and validation of our research model in a social network (e.g., in our prototype of a social network called PESEDIA[3] (Alemany, 2016)). The research model will be used to automatically compute privacy policies during disclosure decisions in social networks. We will test our privacy mechanisms based on the validated model versus other privacy mechanisms considered in the literature. For future research, it would also be interesting to test our research model with OSN users that have already had negative experiences when disclosing personal information on social networks. This would include analyzing a target population with more experience with privacy risks in order to confirm whether or not our hypotheses are also supported. In addition, future studies can extend the current study by including additional constructs that have not been evaluated in the current research, such as risk aversion, general risk, ease of use, and an expansion of message and receiver properties.

7. Conclusion

The goal of the current research was to evaluate the relationship between the elements of online communication (especially channel, message, and receiver), personal information disclosure, and privacy trade-off in the social network context. Based on the literature, a research model was derived and tested using the responses of a study that assesses the constructs of that model. The results revealed a change in privacy trade-off perceptions and their influence on disclosure behaviors with different properties/factors of the elements of communications such as the social circles of receivers, the sensitivity of the message, and the trust in the OSN provider or in other users. While most of the users' perceptions mainly influenced social capital building, there were some significant relationships between family members and unknown relationships that had negative effects on social capital building. In the case of family members there were also repercussions on their privacy concerns. As we predicted, there was no relationship between the message or receivers; however, there was a decrease in users' perceived risk in the case of channel trust and control perception. Last, we confirm that users' perceptions of benefit and risk were properly aligned with their online social well-being. With the extension of privacy trade-off in users' privacy decision-making in social networks, the current research established varying effects of the relationships to different elements of online communication, creating a strong foundation for future studies in privacy decision-making research.

A. Measurement instrument

B. Descriptive statistics, reliability and validity results

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.

Alemany, J. (2016). Pesedia. red social para concienciar en privacidad. Master's thesis, Universitat Politècnica de València, Valencia, Spain.

Alemany, J., del Val, E., Alberola, J., and García-Fornes, A. (2018). Estimation of privacy risk through centrality metrics. *Future Generation Computer Systems*, 82:63–76.

Alemany, J., Del Val, E., and García-Fornes, A. (2020). Empowering users regarding the sensitivity of their data in social networks through nudge mechanisms. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*, pages 2539–2548.

Bakshy, E., Hofman, J. M., Mason, W. A., and Watts, D. J. (2011). Everyone's an influencer: quantifying influence on twitter. In *Proceedings of the fourth ACM international conference on Web search and data mining*, pages 65–74.

Bazarova, N. N. (2012). Public intimacy: Disclosure interpretation and social judgments on Facebook. *Journal of Communication*, 62(5):815–832.

Bennet, A. and Bennet, D. (2008). The decision-making process in a complex situation. In *Handbook on Decision Support Systems 1*, pages 3–20. Springer.

Bourdieu, P. (1985). The forms of capital. *Handbook of Theory and Research for the Sociology of Education*, pages 241–258.

Chang, C.-W. and Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, 30:79–86.

[3] Official project website: https://pesedia.webs.upv.es/

Chen, J. and Shen, X.-L. (2015). Consumers' decisions in social commerce context: An empirical investigation. *Decision Support Systems*, 79:55–64.

Chen, R., Wang, J., Herath, T., and Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems*, 52(1):73–81.

Cheng, J., Adamic, L., Dow, P. A., Kleinberg, J. M., and Leskovec, J. (2014). Can cascades be predicted? In *Proceedings of the 23rd international conference on World wide web*, pages 925–936.

Cheung, C., Lee, Z. W., and Chan, T. K. (2015). Self-disclosure in social networking sites. *Internet Research*.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling.

Choi, B., Wu, Y., Yu, J., and Land, L. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management.

Choi, B. C., Jiang, Z., Xiao, B., and Kim, S. S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, 26(4):675–694.

Church, E. M., Thambusamy, R., and Nemati, H. (2017). Privacy and pleasure: A paradox of the hedonic use of computer-mediated social networks. *Computers in Human Behavior*, 77:121–131.

Davis, J. L. and Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. *Information, communication & society*,

Construct	Code	Items
Privacy Concern (Xu et al., 2013)	PC1	I am concerned that Facebook is collecting too much personal information about me.
	PC2	I am concerned that unauthorized people may access my personal information.
	PC3	I am concerned that Facebook may keep my personal information in an inaccurate manner.
	PC4	I am concerned about submitting personal information to Facebook.
	PC5	It bothers me when Facebook asks me for this much personal information.
Trust in Facebook (Krasnova et al., 2010; Malik et al., 2016)	TF1	I believe that privacy of my personal information is well protected by Facebook.
	TF2	I believe that Facebook will not use my personal information for any other purpose.
	TF3	I believe that Facebook is a secure platform for sharing my personal information.
Perceived Control (Krasnova et al., 2010; Cheung et al., 2015)	CN1	I feel in control over the information I provide on Facebook.
	CN2	I feel in control over who can view my information on Facebook.
	CN3	Privacy settings allow me to have full control over the personal information I provide on Facebook.
Bonding Social Capital (Williams, 2006; Ellison et al., 2007; Church et al., 2017)	BO1	There are people on Facebook I trust to help solve my problems.
	BO2	There are people on Facebook I can turn to for advice about making very important decisions.
	BO3	There are people on Facebook I can talk to when I feel lonely.
	BO4	The people I interact with on Facebook would put their reputation on the line for me.
	BO5	The people I interact with on Facebook would be good job references for me.
	BO6	The people I interact with on Facebook would help me fight an injustice.
	BO7	There is no one on Facebook that I feel comfortable talking to about intimate personal problems. (reversed)
	BO8	There is no one on Facebook I know well enough to get them to do anything important. (reversed)
Bridging Social Capital (Williams, 2006; Ellison et al., 2007; Church et al., 2017)	BR1	Interacting with people on Facebook makes me interested in things that happen outside of my close contacts.
	BR2	Interacting with people on Facebook makes me want to try new things.
	BR3	Interacting with people on Facebook makes me interested in what people unlike me are thinking.
	BR4	Interacting with people on Facebook makes me curious about other places in the world.
	BR5	Interacting with people on Facebook makes me feel like part of a larger community.
	BR6	Interacting with people on Facebook makes me feel connected to the bigger picture.
	BR7	Interacting with people on Facebook reminds me that everyone in the world is connected.
	BR8	On Facebook, I am willing to spend time to support general community activities.
	BR9	Interacting with people on Facebook gives me new people to talk to.
	BR10	On Facebook, I come in contact with new people all the time.
Depth Disclosure (by receiver type), adapted from Wheeless and Grotz (1976), Jiang et al. (2013), and Huang (2016)	DR1	With receiver on Facebook, I intimately disclose who I really am, openly and fully in my conversations.
	DR2	With receiver on Facebook, once I get started, my self-disclosures last a long time.
	DR3	With receiver on Facebook, I typically reveal information about myself without intending to.
	DR4	With receiver on Facebook, once I get started, I intimately and fully reveal myself in my self-disclosures.
Online Social Well-being (Huang, 2016)	SW1	In my Facebook social life, in most respects, I am close to my ideal.
	SW2	In my Facebook social life, the conditions are excellent.
	SW3	In my Facebook social life, I am satisfied.
	SW4	In my Facebook social life, so far, I have obtained the important things I want.
	SW5	In my Facebook social life, if I could live it over, I would change almost nothing.

17(4):476–485.

Construct	Item	Mean	SD	Skew	Kurt	Loadings	AVE	CR	CA
Privacy Concern	PC1	3.87	1.14	-0.65	-0.61	.820	.689	.917	.887
	PC2	3.62	1.12	-0.42	-0.59	.801			
	PC3	3.36	1.21	-0.25	-0.84	.782			
	PC4	3.75	1.09	-0.59	-0.45	.810			
	PC5	3.88	1.09	-0.74	-0.33	.812			
Trust in Facebook	TF1	2.27	1.03	0.37	-0.77	.775	.759	.904	.841
	TF2	2.05	1.09	0.74	-0.42	.831			
	TF3	2.15	1.04	0.47	-0.80	.758			
Perceived Control	CN1	3.02	1.15	-0.11	-0.93	.834	.698	.874	.785
	CN2	3.03	1.07	-0.16	-0.79	.801			
	CN3	3.07	1.05	-0.17	-0.71	.738			
Bonding Social Capital	BO1	2.56	1.17	0.30	-0.84	.809	.515	.889	.859
	BO2	2.52	1.21	0.30	-0.97	.819			
	BO3	2.92	1.31	-0.06	-1.22	.746			
	BO4	2.20	1.06	0.58	-0.46	.681			
	BO5	2.42	1.16	0.42	-0.79	.589			
	BO6	2.72	1.08	0.18	-0.67	.681			
	BO7*	3.56	1.27	-0.54	-0.78	.600			
	BO8*	3.73	1.14	-0.62	-0.44	.532			
Bridging Social Capital	BR1	3.16	1.06	-0.19	-0.61	.784	.542	.922	.906
	BR2	2.93	1.09	0.08	-0.69	.723			
	BR3	2.88	1.09	0.07	-0.63	.714			
	BR4	3.37	1.08	-0.27	-0.60	.693			
	BR5	2.87	1.20	0.11	-0.97	.786			
	BR6	2.88	1.14	0.08	-0.81	.791			
	BR7	3.29	1.14	-0.25	-0.71	.652			
	BR8	2.32	0.99	0.36	-0.55	.655			
	BR9	2.60	1.18	0.22	-1.05	.728			
	BR10	2.30	1.07	0.74	-0.08	.636			
Dept-Disclosure:	DT1	2.43	1.15	0.41	-0.76	.870	.733	.916	.877
Trusted receiver	DT2	2.27	1.08	0.57	-0.44	.859			
	DT3	2.11	1.02	0.70	-0.19	.766			
	DT4	2.27	1.09	0.51	-0.66	.922			
Dept-Disclosure:	DI1	1.65	0.93	1.32	0.95	.859	.667	.889	.832
Influencer receiver	DI2	1.65	0.92	1.36	1.14	.772			
	DI3	1.56	0.79	1.41	1.80	.742			
	DI4	1.49	0.86	1.87	2.96	.885			
Dept-Disclosure:	DF1	2.57	1.16	0.30	-0.82	.872	.727	.914	.874
Friend receiver	DF2	2.37	1.06	0.36	-0.60	.865			
	DF3	2.21	1.03	0.58	-0.26	.762			
	DF4	2.38	1.10	0.37	-0.77	.906			
Dept-Disclosure:	DA1	2.72	1.32	0.12	-1.20	.906	.786	.936	.908
Family receiver	DA2	2.43	1.21	0.42	-0.89	.897			
	DA3	2.25	1.16	0.61	-0.59	.810			
	DA4	2.54	1.28	0.26	-1.14	.931			
Dept-Disclosure:	DC1	1.60	0.87	1.51	2.02	.905	.777	.933	.904
Coworker receiver	DC2	1.64	0.94	1.46	1.45	.833			
	DC3	1.49	0.75	1.43	1.27	.850			
	DC4	1.53	0.80	1.49	1.77	.934			
Dept-Disclosure:	DU1	1.20	0.58	3.58	14.1	.918	.705	.905	.857
Unknown receiver	DU2	1.33	0.82	3.04	9.45	.734			
	DU3	1.24	0.57	2.68	7.45	.791			
	DU4	1.21	0.60	3.38	12.1	.902			
Online Social Well-being	SW1	3.01	1.03	-0.39	-0.47	.813	.663	.907	.874
	SW2	2.96	0.90	-0.27	-0.08	.779			
	SW3	3.34	0.99	-0.75	-0.01	.815			
	SW4	3.11	1.00	-0.52	-0.40	.802			
	SW5	2.96	1.07	-0.20	-0.91	.750			

Note: SD=standard deviation; CR=composite reliability; CA=Cronbach's Alpha; AVE=average variance extracted. *responses reversed prior to evaluation.

Derlega, V. J. and Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3):102–115.

Dunbar, R. (2010). *How many friends does one person need?: Dunbar's number and other evolutionary quirks*. Faber & Faber.

Ellison, N. B., Steinfield, C., and Lampe, C. (2007). The benefits of Facebook "friends:" social capital and college students' use of online social network sites. *Journal of computer-mediated communication*, 12(4):1143–1168.

Esterling, B. A., L'Abate, L., Murray, E. J., and Pennebaker, J. W. (1999). Empirical foundations for writing in prevention and psychotherapy: Mental and physical health outcomes. *Clinical psychology review*, 19(1):79–96.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1):39–50.

Gable, S. L., Reis, H. T., Impett, E. A., and Asher, E. R. (2004). What do you do when things go right? the intrapersonal and interpersonal benefits of sharing positive events. *Journal of personality and social psychology*, 87(2):228.

Galeotti, A. and Goyal, S. (2009). Influencing the influencers: a theory of strategic diffusion. *The RAND Journal of Economics*, 40(3):509–532.

Granovetter, M. S. (1977). The strength of weak ties. In *Social networks*, pages 347–367. Elsevier.

Guo, J., Li, N., Wu, Y., and Cui, T. (2020). Examining help requests on social networking sites: Integrating privacy perception and privacy calculus perspectives. *Electronic Commerce Research and Applications*, 39:100828.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., et al. (1998). *Multivariate data analysis*, volume 5. Prentice hall Upper Saddle River, NJ.

Hallam, C. and Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68:217–227.

Houghton, D., Joinson, A. N., Caldwell, N., and Marder, B. (2013). Tagger's delight? disclosure and liking behaviour in Facebook: the effects of sharing photographs amongst multiple known social circles. Technical report, Birmingham Business School Discussion Paper Series.

Huang, H.-Y. (2016). Examining the beneficial effects of individual's self-disclosure on the social network site. *Computers in human behavior*, 57:122–132.

Huang, L. V. and Liu, P. L. (2017). Ties that work: Investigating the relationships among coworker connections, work-related Facebook utility, online social capital, and employee outcomes. *Computers in Human Behavior*, 72:512–524.

Isaak, J. and Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8):56–59.

Jiang, Z., Heng, C. S., and Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24(3):579–595.

Kasavana, M. L., Nusair, K., and Teodosic, K. (2010). Online social networking: redefining the human web. *Journal of hospitality and tourism technology*.

Kim, D. J., Ferrin, D. L., and Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2):544–564.

Kim, M. S. and Kim, S. (2018). Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behavior*, 88:143–152.

Ko, H.-C. and Kuo, F.-Y. (2009). Can blogging enhance subjective well-being through self-disclosure? *Cyberpsychology & behavior*, 12(1):75–79.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, 11(4):1–10.

Koohikamali, M., French, A. M., and Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, 119:46–59.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, 25(2):109–125.

Krasnova, H. and Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences*, pages 1–10. IEEE.

Lee, H., Park, H., and Kim, J. (2013). 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. *International Journal of Human-Computer Studies*, 71(9):862–877.

Liu, D. and Brown, B. B. (2014). Self-disclosure on social networking sites, positive feedback, and social capital among Chinese college students. *Computers in Human Behavior*, 38:213–219.

Malik, A., Hiekkanen, K., Dhir, A., and Nieminen, M. (2016). Impact of privacy, trust and user activity on intentions to share Facebook photos. *Journal of Information, Communication and Ethics in Society*.

Myers, S. A., Zhu, C., and Leskovec, J. (2012). Information diffusion and external influence in networks. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 33–41.

Nahapiet, J. and Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of management review*, 23(2):242–266.

Nguyen, M., Bin, Y. S., and Campbell, A. (2012). Comparing online and offline self-disclosure: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 15(2):103–111.

Niederhoffer, K. G. and Pennebaker, J. W. (2002). Sharing one's story: On the benefits of writing or talking about emotional experience. *The Oxford Handbook of Positive Psychology*.

Niederhoffer, K. G. and Pennebaker, J. W. (2009). Sharing one's story: On the benefits of writing or talking about emotional experience.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization science*, 5(1):14–37.

Oeldorf-Hirsch, A. and Sundar, S. S. (2015). Posting, commenting, and tagging: Effects of sharing news stories on Facebook. *Computers in human behavior*, 44:240–249.

Park, N., Kee, K. F., and Valenzuela, S. (2009). Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *CyberPsychology & Behavior*, 12(6):729–733.

Peer, E., Brandimarte, L., Samat, S., and Acquisti, A. (2017). Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal*

of Experimental Social Psychology, 70:153–163.

Ponte, E. B., Carvajal-Trujillo, E., and Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management*, 47:286–302.

Quah, E. and Haldane, J. (2007). *Cost-benefit analysis*. Routledge.

Quan-Haase, A. and Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology & Society*, 30(5):350–361.

Schiffrin, H., Edelman, A., Falkenstern, M., and Stewart, C. (2010). The associations among computer-mediated communication, relationships, and well-being. *Cyberpsychology, Behavior, and Social Networking*, 13(3):299–306.

Squicciarini, A. C., Paci, F., and Sundareswaran, S. (2014). Prima: a comprehensive approach to privacy protection in social network sites. *annals of telecommunications-annales des télécommunications*, 69(1-2):21–36.

Such, J. M., Porter, J., Preibusch, S., and Joinson, A. (2017). Photo privacy conflicts in social media: A large-scale empirical study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3821–3832. ACM.

Sun, Y., Wang, N., Shen, X.-L., and Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52:278–292.

Sylaska, K. M. and Edwards, K. M. (2014). Disclosure of intimate partner violence to informal social support network members: A review of the literature. *Trauma, Violence, & Abuse*, 15(1):3–21.

Taddei, S. and Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3):821–826.

Tidwell, L. C. and Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human communication research*, 28(3):317–348.

Vitak, J. and Ellison, N. B. (2013). "there's a network out there you might as well tap": Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media & Society*, 15(2):243–259.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., and 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*, pages 1–16.

Wellman, B. and Wortley, S. (1990). Different strokes from different folks: Community ties and social support. *American journal of Sociology*, 96(3):558–588.

Wheeless, L. R. and Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human communication research*, 2(4):338–346.

Williams, D. (2006). On and off the'net: Scales for social capital in an online era. *Journal of computer-mediated communication*, 11(2):593–628.

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

Xu, H., Dinev, T., Smith, H. J., and Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, page 6.

Xu, H., Teo, H.-H., Tan, B. C., and Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 23(4):1342–1363.

Yang, M., Yu, Y., Bandara, A. K., and Nuseibeh, B. (2014). Adaptive sharing for online social networks: A trade-off between privacy risk and social benefit. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 45–52. IEEE.