Computers in Human Behavior 69 (2017) 302–310

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

COMPUTERS IN HUMAN BEHAVIOR

Full length article

Privacy concerns on social networking sites: Interplay among posting types, content, and audiences

Yongick Jeong [a], [*], Yeuseung Kim [b]

[a] Louisiana State University, Manship School of Mass Communication, 211 Journalism Building, Baton Rouge, LA 70803, USA
[b] DePaul University, College of Communication, 1 E Jackson Blvd., Chicago, IL 60604, USA

ARTICLE INFO

Article history:
Received 23 July 2016
Received in revised form
20 October 2016
Accepted 18 December 2016
Available online 19 December 2016

Keywords:
Privacy concerns on social networking sites (SNS)
Content shared on social media
Posting types
Facebook
Twitter

ABSTRACT

This study examines the impact of the types of posting, information types, and privacy concerns toward audience types across two types of social networking sites (SNSs), Facebook and Twitter. The findings indicate that on Facebook, young SNS users are more concerned about other users posting on their own timeline than other types of posting. On Twitter, young SNS users are more concerned about their own tweets than other users retweeting their tweets. The study also found that different content within different posting types has varying influence on privacy concerns constructed by the user based on three audience types (marketer, authoritative, distant relations). Implications for policy-making and suggestions for future research are discussed.

1. Introduction

According to the Pew Research Center, 65% of Internet users in the U.S. use at least one social networking site (SNS) (Perrin, 2015). Across demographic groups, young adults (ages 18 to 29) are the heaviest users of SNS—87% report using Facebook, 37% use Twitter, and 53% use Instagram (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015). One of the primary reasons for the widespread popularity of SNSs is the easy production and reproduction of content, such as information about one's location, personal activities, and time spent with others. In addition, SNS users are able to share information at a mass scale with their connections, i.e., friends and followers. For instance, Facebook users can post information on their own timelines to share information with everyone in their network and write on friends' timelines to share with their friends' networks.

Scholars have been examining the privacy issues of SNSs, even at the embryonic stage of SNSs (Bergström, 2015; Debatin, Lovejoy, Horn, & Hughes, 2009; Hampton, Goulet, Marlow, & Rainie, 2012; Hoy & Milne, 2010; Kim, 2016; Waters & Ackerman, 2011). Privacy is expected to exert greater influence on how people behave on SNSs as more people become familiar with using SNSs to share information about themselves. The open platforms of SNSs often allow users outside the social network to openly access information shared on SNSs, unless a user imposes strict privacy settings. Privacy is a complex concept that is frequently regulated by people depending on the context (Altman, 1975), the type of information shared, and the degree of intimacy of the social circle, ranging from family and close friends to those who are acquainted through distant relations. Considering how SNSs are consumed as key media, especially among young adults, more research is required to have a better understanding of privacy concerns and how users' behaviors are affected by it.

Disclosing information on SNSs can take place in multiple ways. For example, Twitter users can tweet their information and share others' information by retweeting their tweets, while other users can also share users' tweets through the retweeting feature. Facebook users can post on their own timelines and post on friends' timelines, while friends can post on other users' timelines. Therefore, this study seeks to understand the multidimensional nature of privacy concerns on SNSs by examining the type of content shared on SNSs (e.g., location, action, social, general, and personal information), the type of potential audiences for the shared content (e.g., authoritative figures, marketers, and those in distant relations), and the types of posting (e.g., postings on own SNS, posting on others'

[*] Corresponding author.
E-mail addresses: yjeong@lsu.edu (Y. Jeong), y.kim@depaul.edu (Y. Kim).

http://dx.doi.org/10.1016/j.chb.2016.12.042
0747-5632/© 2016 Elsevier Ltd. All rights reserved.

SNS, or others' postings on one's own SNS) across two popular SNSs, Facebook and Twitter. The findings of this study will contribute to a more technical understanding of the multidimensional nature of privacy issues on SNSs and provide guidelines for developing relevant privacy policies on SNSs.

2. Literature review

2.1. SNSs: uses and gratifications approach

The various types of SNSs serve different purposes for Internet users due to their structural differences and thus, a user's motivation for using SNSs determines which site they decide to use (Johnson & Yang, 2009). Facebook is an example of a traditional form of SNS, which is an online platform that enables users to create personal profiles, share information with friends and connections, and make and provide lists of those connections (Boyd & Ellison, 2007). Twitter is an example of a microblogging SNS: a blog style platform that enables users to share smaller bits of information with other members interested in similar topics (Johnson & Yang, 2009).

Using the uses and gratifications approach, researchers provide insights into individual motivations for using SNSs and the expected outcomes of using SNSs (e.g., Raacke & Bonds-Raacke, 2008; Ruggiero, 2000). There are several benefits of SNSs that motivate users to stay active. For example, a focus group of college students revealed that Facebook fulfills five primary needs of an Internet user: communication, convenience, curiosity/information seeking, popularity, and maintaining/building relationships (Urista, Dong, & Day, 2009). Similarly, Acquisti and Gross (2006) identified communication, curiosity, and convenience as motivations for college students' use of Facebook, while other researchers detected entertainment as a chief motivator for using SNSs among college students (Ezumah, 2013; Waters & Ackerman, 2011). Social connectedness is another motivation identified as a reason people use Facebook (Alloway & Alloway, 2012). Research concerning microblogging SNSs such as Twitter had similar findings. For example, one study found that the need for connection is the most important factor in using Twitter (Chen, 2011), and by monitoring the Twitter followers of a retired female, another study identified five primary factors in using microblogging SNSs: communication, information, entertainment, convenience, and commerce (Clavio & Kian, 2010). Overall, the need for communication seems to be the most important factor when using SNSs.

Some studies have observed the different purposes of using Facebook versus Twitter among young adults and found that young adults use Facebook more than Twitter for communication and convenient needs (Jeong & Coyle, 2014). In terms of privacy concerns, young SNS users are more concerned about information on Facebook than on Twitter when worrying about information exposure by authority figures (e.g., parents, coworkers, bosses, and teachers) than those in distant relations (e.g., friends of friends, acquaintances, and strangers) (Jeong & Coyle, 2014).

2.2. Privacy on SNSs

Individuals have a reasonable desire to keep aspects of their lives private in order to maintain certain standards for their various types of relationships (Rachels, 1975). Privacy can be conceptualized as the ability to be free from unwanted intrusions, and to maintain their privacy, individuals go through a personal boundary regulation process to regulate the levels of privacy with others (Zlatolas, Welzer, Heričko, & Hölbl, 2015). The two key concepts that determine one's privacy are accessibility and control (Rachels, 1975). Accessibility is the ease by which others can attain one's private information while control is the ability for an individual to establish and maintain boundaries around their information, letting in whom they want and keeping out those they do not want. An individual's ability to create and maintain personal relationships with others is related to that individual's ability to control who has access to their personal information. Thus, privacy is essential to maintaining the different types of relationships people prefer to have with others. Rachels (1975) argues that for individuals to maintain control of their relationships, they must have control over who has access to them.

Visibility is another widely discussed concept in regards to SNS privacy (Fox & Moreland, 2015). Visibility refers to the ease by which other people can see your profile, information, or posts. Generally, the less privacy control users have, the more visible they are to other users. SNSs offer connectivity and association, giving users the ability to view each other's profiles through direct connection or through a common connection. This means that in current SNS settings, especially on Facebook, user information may be visible not only to their friends, but to those who have a friend relationship with their friends as well. Thus, under current SNS settings, visibility grants access to users' profile without their knowledge. As a result, those whom users may not have wanted to share their information with could gain access to that information (Fox & Moreland, 2015). This unwanted privacy breach could occur even with the most restricted privacy settings. For example, even though a user has control over his or her own account, when the user's Facebook friends have different, less restricted privacy settings, the user's information and posts could be visible to more people than the user initially anticipated (Tan, Qin, Kim, & Hsu, 2012). Furthermore, information that is posted to SNSs can be accessible even after the post is removed due to the ease at which information can be saved, shared, and reposted (Fox & Moreland, 2015). This lack of control over activity streams is identified as one of the privacy-sensitive areas on SNSs (Fox & Moreland, 2015). Here, the activity stream is referred to as the feed that shows all of a particular user's activities (e.g., posts and likes). For instance, a user might not be aware of all the events that are added to their activity stream, nor who has access to their activity stream (Fox & Moreland, 2015). Hence, inability to effectively regulate who has access to one's information online can create concerns for SNS users.

2.3. Threat to privacy on SNSs

The interactive nature of SNSs allows advertisers and marketers to easily engage with their consumers. Advertisers and marketers can provide direct responses to consumers and provide personalized information. For instance, Facebook implemented a platform for programs created by third-party developers that allowed applications to track user behaviors and made information from personal accounts available for targeted advertising (Debatin et al., 2009). This raises concerns of privacy for SNS users. These concerns are social in nature, such as an inadvertent disclosure of personal information when a consumer interacts with a piece of content (e.g., “like” a post), then that interaction becoming visible in the newsfeed or on a consumer's timeline (Lipsman, Mudd, Rich, & Bruich, 2012). Some SNS users may be concerned about damaging reputations due to gossip and rumors (Debatin et al., 2009). Other concerns associated with Facebook use include the fear of unwanted contact, harassment or stalking, hacking, identity theft, and worries about Facebook's allowance of third parties to access personal data (Debatin et al., 2009).

Although SNS users may raise concerns about their privacy on SNSs, past studies have found that the degree of perceived concern for privacy is not directly associated with users' intentions to use

SNSs. Despite their reported concerns, user attitudes toward SNSs seems to remain positive. Some call this disconnect between a user's desire to keep their information private and their actual privacy settings on SNS “privacy paradox” and suggest that consumer privacy might not be such a hindrance for using SNSs (e.g., Dienlin & Trepte, 2014; Taddicken, 2014; Tan et al., 2012). Although users might cognitively acknowledge their concern for privacy, behaviorally, they are not too guarded or careful about revealing information about themselves.

Another puzzling concept is the idea of voluntarism, which is the willingness to publicize personal information, despite being fully aware of the potential hazardous consequences (Blatterer, 2010). One reason for this disconnect lies in a user's desire for visibility and affirmation. Even though there is concern about unintended viewers being able to see one's information, there is a simultaneous desire to be seen and admired by as many users as possible, especially among teens and young adults. Based on a survey with over 4000 college students, Tan et al. (2012) found that only a small percentage of students actually changed their privacy preferences despite potential attacks on privacy. Blatterer (2010) argues that this strong desire to disclose information for attention or heightened visibility is a result of self-identity and individualization. Debatin et al. (2009) also found that despite considerable threat to personal privacy, user gratification of pleasure or satisfaction gained from using SNSs outweighed perceived threats to privacy. Similarly, Roberts (2010) detected that although users modified their privacy settings due to overwhelming privacy concerns, college students were generally less concerned about marketing efforts using their private information on SNSs.

Individuals may also be willing to jeopardize their privacy because they are concerned about being forgotten and left alone. This phenomenon is called fear of missing out (FoMO). Particularly among young adults, there is the strong need to stay connected via SNSs despite stressors in order to avoid being left out and to maintain relationships (Fox & Moreland, 2015). FoMO is characterized as an anxious feeling that others are sharing enjoyable experiences. As a result of strong disdain of FoMO, young SNS users attempt to stay constantly connected and updated on what other peers are doing. Thus, although young adults are aware of potential privacy breaches, their desire to be a part of their peers' activities outweigh those concerns when using SNSs.

2.4. Theoretical understanding of privacy on SNSs

Westin (1967) argues that privacy is one of the several needs that assist individuals in their emotional adjustment to daily interpersonal interactions. Westin (1967) identified four levels of privacy: solitude, intimacy, anonymity and reserved. Solitude is freedom from observation by others, while intimacy is characterized by a small group of individuals who are secluded from others to develop their personal relationships. Anonymity is freedom from identification or surveillance in public spaces. Finally, being reserved is limiting disclosure to others in a way that others know that you are avoiding disclosure. These desires come at different times, in different situations, and differently for different relationships. Westin (1967) asserts that people achieve their privacy through these levels. Thus, without their application to the relationships, desired privacy cannot be attained (Margulis, 2011). Additionally, Westin (1967) discusses the purposes of privacy in three ways. The first is personal autonomy, which is the desire to avoid manipulation, domination, or exposure by other individuals. Limited communications are interpersonal boundaries set in order to protect one's privacy. Finally, protected communication indicates the ability to share information with certain individuals while withholding that information from others.

Rachels (1975) explains the privacy theory with regards to social interactions and personal relationships. Disclosing personal and private information is more appropriate for some relationships (e.g., family members or close friends) than others (e.g., co-workers, supervisors or other business relationships) unless there is a reason to reveal information to the latter group of people. If individuals are unable to control or restrict access to certain relationship groups, they may not be able to engage in the specific behaviors necessary for that relationship (Mooradian, 2009). For example, being able to disclose information to a close friend that you do not disclose to the general public is an important function of friendship. Once it has been disclosed to everyone else, it loses its value within the friendship. As some relationships are based on an exchange of information that is considered exclusive and selective, individuals should be able to control the exchange of their personal information for the sake of their relationships (Rachels, 1975). Therefore, in order to cultivate personal relationships with others, individuals control and even restrict access to their information.

This in-group (i.e., those in close relationships or those who share the same identity) and out-group (i.e., those in distant relationship or those who do not share the same identity) notion has been discussed when examining privacy issues on SNSs (Bergström, 2015; Hebl, Williams, Sundermann, Kell, & Davies, 2012; Thelwall, 2011). General findings indicate that SNS users are more likely to be friends with and interact with in-group members than out-group members (Hebl et al., 2012), trust in-group members more than out-group users, and share information more comfortably within in-group connections while being more concerned about misuse of their personal information by out-group connections (Bergström, 2015). Hebl et al. (2012) investigated racial intergroup contact on Facebook and found that users are more likely to recognize friends who are perceived to belong to the same racial identity as their in-group. A similar pattern was also detected in LGBT users, who tended to take deliberate measures to avoid friendship with out-group members on SNSs (Thelwall, 2011).

Communication privacy management theory provides an overarching framework for how individuals control privacy: essentially, self-disclosure is an individual's balancing act where individuals develop their own rules to make decisions about revealing or concealing private information (Frampton & Child, 2013; Metzger, 2007). Without certain personal rules and restrictions on one's privacy, one can lose control of their relationships (Rachels, 1975). Privacy boundaries set by an individual can range from completely open to completely closed (Petronio, 2002). Completely open boundaries are characterized by a willingness to disclose information verbally or online to anyone who wants access, representing a process of revealing. In contrast, closed boundary individuals are cautious about their information and make sure that their information is not accessible through a process of concealing and protecting. People typically go back and forth between open and closed boundaries, depending on various factors such as relationship, context, and users' personal criteria (Margulis, 2011; Petronio, 2002).

3. Research questions

In order to gain a better understanding of privacy concerns involved in the types of information, posting types, and privacy concern types on SNS, this study examines two types of SNS (Facebook and Twitter) for the following reasons: First, they are the most popularly used SNSs among young adults. Second, in terms of functional difference, Facebook is categorized as a traditional SNS, where users share information with other users by posting information on one's timeline but also on others' timelines, while

Twitter is categorized as a microblogging SNS, where the users typically post information on their own personal account (Jeong & Coyle, 2014). As there is lack of research examining various types of information by the type of posting behaviors and how they might each affect privacy concerns, this study asks the following questions:

RQ1. Do SNS users show varying levels of concern for privacy for different types of posting activities (i.e., one's own posting on own timeline, one's posting on other's timeline, others posting on one's own timeline) on Facebook and Twitter?

RQ2. How do the types of information (i.e., location, action, social, general, personal information) and types of posting activities (i.e., one's own posting on own timeline, own posting on others' timelines, others posting on one's own timeline) influence privacy concerns for various types of audiences (marketers, authoritative relations, and distant relations) on Facebook and Twitter?

4. Method

4.1. Participants

A total of 216 college students from a large university in the Southern U.S. participated in the study for extra credit. The participants were chosen from the mass communication research pool where the students were enrolled for different mass communication courses. Students are able to freely choose the study they are interested in: thus, no participant was asked to participate against their interest. The mean age was 20 years old and 71.76% of the participants were female. An online survey link was sent to students who volunteered to participate. Initially, a total of 221 students responded to the survey. Among the 221 responses, five surveys containing less than 80% of responses for key measures were eliminated from the analyses. While all 216 participants reported having a working Facebook account, 175 participants currently owned an active Twitter account.

4.2. Measures

The types of content users share on SNSs, the different types of posting activities, and the different types of audience were measured.

4.2.1. Types of information posts on SNSs

Participants were asked to rate their likelihood of disclosing five types of content on Facebook and Twitter on a scale ranging from 1 “not at all likely” to 7 “very likely”: location-based posts (i.e., where you are), action-oriented posts (i.e., what you are engaged in), social activity posts (i.e., who you spend time with), general information posts (i.e., general posts about news, sports, other public affairs, etc.), and personal information posts (i.e., personal relationships or personal events) (Jeong & Coyle, 2014).

4.2.2. Privacy concern by the types of posting activities

In order to capture all types of behavior that may be associated with individual user privacy on SNSs, this study focused on posting activities rather than viewing activities of one's own and others' postings. Thus, considering the various places a user can post on Facebook and the various ways a piece of information can be shared on Twitter, the five types of information identified above were assessed in three ways. For Facebook, postings on the user's own timeline, the user's postings on other users' timeline, and other users' postings on the user's own timeline. For Twitter, the user's own tweets, the user's retweets of others' tweets, and other users' retweets of the user's tweets. A seven-point semantic differential scale, ranging from 1 “not at all likely” to 7 “very likely,” was used to measure the likelihood of posting each information type.

Using this classification, the perceived privacy concern was measured for each posting activity. For Facebook, privacy concerns about the user's posting on their own timeline, posting on other users' timeline, and other users' postings on the user's own timeline were measured. For Twitter, the privacy concerns about the user's own tweets, the user's retweets of others' tweets, and others' retweets of the user's tweets were measured on a scale ranging from 1 “not at all concerned” to 7 “very concerned.”

4.2.3. Privacy concern by the types of audiences

For each SNS, concern for privacy regarding the audiences of the disclosed information was measured using a seven-point scale, ranging from 1 “not at all concerned” to 7 “very concerned.” Adopting Jeong and Coyle’s (2014) categorization, three audience types were examined: marketers (e.g., companies, agencies, and advertisers), authoritative figures (e.g., parents, supervisors, coworkers, and teachers), and distant relations (e.g., strangers, acquaintances, and friends of friends).

5. Results

5.1. Univariate analyses

Results showed that participants are generally more concerned about what other users post on their own timeline than both what they post on their own timelines and what they post on other users' timelines on Facebook. On Twitter, participants worried more about what they tweeted than what they retweeted (of others' tweets) or what others retweeted from their own tweets. In terms of privacy concerns, participants were more concerned about authoritative figures, regardless of SNS type. The descriptive statistics of major variables are displayed in Table 1.

5.2. Perceived concern for privacy by the types of posting activities on SNSs

RQ1 asked if SNS users have a varying level of perceived concern for privacy regarding the type of information they share on Facebook and Twitter. Repeated measure analyses showed different patterns for the two. For Facebook, perceived concern for privacy was significantly higher for *information other users' post on the user's own timeline* ($M = 4.91$, $SD = 1.94$) than *information the user posts on his or her own timeline* ($M = 4.44$, $SD = 2.20$) and *information the user posts on others' timeline* ($M = 4.26$, $SD = 2.05$), $F(2, 172) = 18.19$, Wilks' $\lambda = 0.83$, $p < 0.001$, $\eta^2 = 0.18$ (see Table 2). For Twitter, users were more concerned about *the user's own tweets* ($M = 3.29$, $SD = 2.32$) than *others retweeting the user's own tweets* ($M = 2.95$, $SD = 2.16$), $F(2, 172) = 4.66$, Wilks' $\lambda = 0.95$, $p < 0.05$, $\eta^2 = 0.05$ (see Table 3).

5.3. Impact of the types of information and posting activities on perceived privacy threats

To examine whether the perceived privacy concerns for various audience types (general concern for SNS privacy, marketers, authoritative figures, and distant relations) was influenced by the types of information and posting behaviors on Facebook and Twitter, a series of hierarchical regression analyses were performed.

For Facebook, the five types of information (location, action, social, general, and personal information) SNS users provided on their own timeline were entered into the first block. Then, the

Table 1
Univariate analysis of major variables by SNS types.

		Mean	SD	Min	Max	Skewness	Kurtosis
Privacy concerns based on posting types on Facebook (n = 216)	Own posting own timeline	4.43	2.19	1	7	−0.38	−1.31
	Own posting on others' timeline	4.26	2.04	1	7	−0.30	−1.15
	Others' posting on own timeline	4.91	1.94	1	7	−0.75	−0.54
Privacy concerns based on posting types on Twitter (n = 175)	My tweets	3.30	2.32	1	7	0.42	−1.40
	My retweets	3.17	2.19	1	7	0.49	−1.26
	Others' retweets of my tweets	2.95	2.16	1	7	0.65	−1.06
Privacy concerns based on audience types on Facebook (n = 216)	Marketers	3.54	1.91	1	7	0.24	−1.01
	Authoritative figures	4.13	2.08	1	7	−0.17	−1.28
	Distant relations	3.49	1.90	1	7	0.21	−1.05
	Overall privacy concern on Facebook	3.72	1.54	1	7	0.05	−0.69
Privacy concerns based on audience types on Twitter (n = 175)	Marketers	2.55	1.89	1	7	1.04	−0.14
	Authoritative figures	3.27	2.25	1	7	0.43	−1.34
	Distant relations	2.61	1.88	1	7	0.96	−0.24
	Overall privacy concern on Twitter	2.81	1.68	1	7	0.62	−0.56

Table 2
Difference in perceived privacy concerns by the types of posting activities on Facebook.

SNS format	My posting on own timeline mean (*SD*)	My posting on others' timeline mean (*SD*)	Others' posting on my timeline mean (*SD*)	Wilks' λ	*F*-value	Partial η^2
Facebook***	4.44 (2.20)$_{A}$	4.26 (2.05)$_{A}$	4.91 (1.94) $_{B}$	0.83	18.19	0.18

Note. [1]: Subscripts next to the mean (standard deviation) indicate significant difference among the type of postings on Facebook in paired-sample *t*-test at a 0.05 significance level (i.e., A < B).
[2]: $^{***}p < 0.001$.

Table 3
Difference in perceived privacy concerns by the types of posting activities on Twitter.

SNS format	My tweets mean (*SD*)	My retweets mean (*SD*)	Others' retweets of my tweets mean (*SD*)	Wilks' λ	*F*-value	Partial η^2
Twitter*	3.29 (2.32)$_{B}$	3.17 (2.19) $_{AB}$	2.95 (2.16) $_{A}$	0.95	4.66	0.05

Note. [1]: Subscripts next to the mean (standard deviation) indicate significant difference among the type of postings on Twitter in paired-sample *t*-test at a 0.05 significance level (i.e., A < B).
[2]: $^{*}p < 0.05$.

information users posted on other users' timelines and the information other users posted on the users' own timelines were entered into the second and third blocks, respectively. The results showed that the various types of information and the types of posting behavior are not significantly associated with the overall perceived privacy threats on Facebook. The total variance explained by Model 1 was 13.2%. The privacy concern for marketers was significantly influenced by other users' posting of *location* information on users' own timeline ($b = 0.53$, $\beta = 0.49$, $p < 0.001$). The privacy concern for authoritative figures was significantly influenced by users' posting of *action* information on their own account ($b = 0.29$, $\beta = 0.28$, $p < 0.05$). The various types of information and the types of posting behavior did not affect privacy concern for distant relations. The total variances explained by Model 2 (marketer privacy concern), Model 3 (authoritative privacy concern) and Model 4 (distant relations privacy concern) are 15.4%, 15.1%, and 9.6%, respectively. The results of multiple regression analyses are shown in Table 4.

Similarly, for Twitter, the types of information users can tweet were entered into the first block. Then, the information users retweeted and users' own tweets that other Twitter users retweeted were entered into the second and third blocks, respectively. The results showed that the user's retweets of *action* information had a positive influence ($b = 0.34$, $\beta = 0.45$, $p < 0.05$) and other users' retweets of the user's *action* tweets had a negative effect ($b = -0.43$, $\beta = -0.51$, $p < 0.05$) on the overall perceived privacy concern on Twitter. The total variance explained by Model 5 was 20.6%. For the marketers' privacy concern on Twitter, other users' retweets of the user's *location* tweets had a positive effect ($b = 0.34$, $\beta = 0.45$, $p < 0.05$) and *action* tweets ($b = -0.44$, $\beta = -0.45$, $p < 0.05$) and *personal information* tweets had negative effects ($b = -0.33$, $\beta = -0.34$, $p < 0.05$). The total variance explained by Model 6 (marketer privacy concern) was 14.2%. For the authoritative privacy concern, the user's retweets of *action* information ($b = 0.41$, $\beta = 0.41$, $p < 0.05$) had a significant effect. The user's retweets of action information also had a positive effect ($b = 0.35$, $\beta = 0.41$, $p < 0.05$) on the distant relation privacy concern along with other users' retweets of the user's *action* tweets ($b = -0.62$, $\beta = -0.65$, $p < 0.001$). The total variances explained by Model 7 (authoritative privacy concern) and Model 8 (distant relations privacy concern) were 18.5% and 24.6%, respectively. The results of multiple regression analyses are shown in Table 5.

6. Discussion

This study examined the multidimensional nature of privacy concern on SNSs by examining the interplay among the five types of content often shared on SNSs (location, action, social, general, and personal), three forms of postings (posting on one's own timeline, posting on other users' timeline, and other users' posting on own timeline), and three types of audiences (concern for marketers, authoritative, and distant relations) using two widely used SNSs, Facebook and Twitter. SNSs are designed in a way that friends of friends can often access users' information (Mooradian, 2009). For example, on Facebook, when a user posts information on one's own timeline, it is typically visible and accessible to the user's “friends” as well. Similarly, when the user posts information on others' timelines, it can be also viewed by other users' friends, expanding

Table 4
Impact of the content types and posting types on privacy concerns on Facebook.

	Model 1	Model 2	Model 3	Model 4
	Facebook privacy concern	Marketers privacy concern	Authoritative privacy concern	Distant relations privacy concern
1. Independent variables				
My posting on own timeline				
Location	−0.14 (−0.16)	−0.19 (−0.18)	−0.14 (−0.12)	−0.09 (−0.08)
Action	0.09 (0.12)	0.13 (0.14)	0.29 (0.28)*	−0.13 (−0.15)
Social	−0.02 (−0.02)	−0.10 (−0.10)	−0.10 (−0.09)	0.14 (0.15)
General	−0.09 (−0.11)	−0.04 (−0.04)	−0.08 (−0.07)	−0.15 (−0.15)
Personal	0.16 (0.19)	0.16 (0.15)	0.11 (0.10)	0.20 (0.20)
My posting on other's timeline				
Location	−0.09 (−0.08)	−0.26 (−0.19)	−0.05 (−0.03)	0.03 (0.02)
Action	0.03 (0.03)	0.12 (0.10)	0.12 (0.09)	−0.14 (−0.12)
Social	0.12 (0.13)	0.11 (0.10)	0.17 (0.14)	0.08 (0.07)
General	0.05 (0.06)	0.02 (0.02)	0.01 (0.01)	0.11 (0.11)
Personal	−0.07 (−0.08)	−0.14 (−0.13)	0.06 (0.05)	−0.14 (−0.13)
Others' posting on my timeline				
Location	0.24 (0.27)	0.53 (0.49)***	−0.04 (−0.04)	0.23 (0.21)
Action	−0.16 (−0.18)	−0.04 (−0.04)	−0.18 (−0.15)	−0.26 (−0.24)
Social	0.10 (0.11)	−0.22 (−0.20)	0.25 (0.21)	0.26 (0.24)
General	0.16 (0.18)	0.22 (0.19)	0.15 (0.12)	0.12 (0.11)
Personal	−0.08 (−0.09)	−0.11 (−0.10)	−0.11 (−0.09)	−0.03 (−0.03)
2. Incremental/Total R^2				
Posting my own (%)	5.5	4.0	8.3	3.3
Posting on others (%)	3.7	2.2	5.3	1.9
Others posting on mine (%)	4.0	9.1	1.4	4.4
Total model	13.2	15.4	15.1	9.6

Note. † Cell entries in section 1 are regression coefficients (standardized beta coefficients are shown in parentheses). (*: $p < 0.05$, ***: $p < 0.001$).

Table 5
Impact of the content types and posting types on privacy concerns on Twitter.

	Model 5	Model 6	Model 7	Model 8
	Twitter privacy concern	Marketers privacy concern	Authoritative privacy concern	Distant relations privacy concern
1. Independent variables				
My tweets				
Location	0.11 (0.15)	0.09 (0.10)	0.15 (0.15)	0.09 (0.11)
Action	0.04 (0.06)	0.11 (0.13)	−0.11 (−0.11)	0.12 (0.14)
Social	0.01 (0.01)	−0.11 (−0.13)	0.19 (0.19)	−0.07 (−0.08)
General	−0.01 (−0.01)	−0.06 (−0.07)	0.01 (0.01)	0.01 (0.01)
Personal	0.14 (0.18)	0.14 (0.16)	0.20 (0.20)	0.08 (0.09)
My retweets of others' tweets				
Location	−0.11 (−0.11)	−0.10 (−0.10)	−0.09 (−0.07)	−0.08 (−0.07)
Action	0.34 (0.45)*	0.25 (0.30)	0.41 (0.41)*	0.35 (0.41)*
Social	0.06 (0.08)	−0.06 (−0.07)	0.08 (0.08)	0.16 (0.19)
General	−0.12 (−0.16)	0.01 (0.01)	−0.16 (−0.16)	−0.22 (−0.27)
Personal	0.04 (0.05)	0.04 (0.04)	−0.05 (−0.05)	0.13 (0.14)
Others' retweets of my tweets				
Location	0.14 (0.14)	0.44 (0.37)*	−0.02 (−0.02)	−0.02 (−0.01)
Action	−0.43 (−0.51)*	−0.44 (−0.45)*	−0.23 (−0.20)	−0.62 (−0.65)***
Social	0.07 (0.09)	0.07 (0.07)	−0.15 (−0.13)	0.30 (0.32)
General	0.09 (0.11)	0.09 (0.10)	0.09 (0.09)	0.09 (0.10)
Personal	−0.17 (−0.19)	−0.33 (−0.34)*	−0.11 (−0.10)	−0.06 (−0.06)
2. Incremental/Total R^2				
Posting my own (%)	8.6	2.2	10.6	6.5
Posting on others (%)	3.2	1.0	2.9	9.1
Others posting on mine (%)	8.8	11.0	5.0	8.9
Total model	20.6	14.2	18.5	24.6

Note. † Cell entries in section 1 are regression coefficients (standardized beta coefficients are shown in parentheses). (*: $p < 0.05$, ***: $p < 0.001$).

the scope of who views the posted information.[1] Thus, in addition to the types of information and audiences, it is also important to understand the impact of posting venues (e.g., my timeline vs. others' timeline) since it determines the potential audience of the disclosed information.

Unless a user is extremely cautious about their privacy settings and chooses to impose strict restrictions on who has access to their shared information—in which case, an SNS would not be the most restricted platform to post on—personal information shared on the Internet will often find its way to unintended recipients. When an individual adds a new friend to their network, often times the new friend's friends are also added to that network, granting them

[1] Current Facebook privacy settings allow detailed control of the information where a user can restrict others' postings on the user's timeline to be viewed only by the user and not by the user's friends, allow it to be viewed by the users' friends only, or allow it to be viewed by others' friends. This information was not revealed to the participants at the time of data collection.

access to the individual's information (Mooradian, 2009). Unknowingly, personal information may be shared with these unintended audiences, and it is almost impossible to retract disclosed information.

RQ1 was proposed to address this question of perceived concern for the potential scope of shared information and whether or not users were consciously aware of what posting on different spaces might imply (sharing on one's own network vs. expanding information to others' network). Results showed that on Facebook, a user is more concerned about others posting something on the user's timeline than when the user is the writer of a post on their own timeline or visiting others' profile to write something on their timeline. This may be because what others post on one's timeline is often uncontrollable. Conversely, on Twitter, users were more concerned about their own tweets than others sharing one's information with others via retweets. This may be because of the structural difference between Facebook and Twitter. As mentioned before, Facebook is an example of a traditional idea of SNS where a community is formed around one's network and social interaction, whereas Twitter focuses more on broadcasting information to the general public and there's an understanding that anyone can view one's tweet.

RQ2 was an attempt to address the issue of which behavior on SNSs might affect various types of privacy concern on SNSs. On Facebook, other people's postings about their location-related information on one's timeline increased privacy concern when the audience was marketers. As many people are using smartphones to access Facebook, exact locations can be easily shared via the check-in feature using geotargeting technology or the GPS system on users' phones. As what others post on one's own timeline is uncontrollable and location is often used to promote events, restaurants, stores and other businesses, users may already be aware that location information provided by others could be used by marketers for targeted promotional services more than other types of information. For example, if a friend leaves information about a visit to a restaurant on another user's timeline, the connected friend indirectly becomes an endorser for the restaurant and advertisers could easily use that piece of information for marketing purposes. Another significant variable was user's own posting of what they are doing and their concern for authoritative figures.

On Twitter, some noteworthy patterns regarding concern for privacy emerged. First, similar to Facebook, other users' retweets of the user's location increased privacy concerns about marketers on Twitter. Again, this may be because users are aware that they could receive targeted promotional messages based on this information. In addition, sharing exact physical location with an unknown network of people might be associated with safety issues. Second, no significant variables regarding one's own tweets could also be explained by the controllability of information. One's own tweets regarding all five types of information are completely under the user's control. If one chooses to tweet about any type of the information, it almost certainly means that the user is aware that anyone with Internet access can view the information. Thus, users do not feel concerned about privacy when tweeting because the act of tweeting will only take place when one is not concerned about privacy. Interestingly, other users' retweets of the user's action-related tweets had a negative effect on the overall perceived privacy concern on Twitter and privacy concerns regarding authoritative figures and distant relations. This means that others' retweets of the user's information further lessens concern for privacy. Perhaps users see retweets as a signal that the retweeted information is of value to others (especially to the person retweeting) rather than a threat to privacy.

Lastly, one unexpected finding was that user's own retweets of action-related information (about others) increased general Twitter privacy concern and privacy concerns regarding authoritative figures and distant relations. This suggests that users experience heightened concern for privacy when they engage in retweeting behavior of other people's action-related tweets. One explanation for this might be that retweeting reveals multiple pieces of information. It suggests that the user not only supports the message in the tweet but also the person who tweeted it and, on top of that, that the user is willing to broadcast it to their own network as well as the general public.

6.1. *Implications, limitations, and future directions*

Despite the significance of the issue and implications on policy-developing, little empirical attempts have been made to understand the multidimensional nature of SNS privacy concerns structured based on the types of information, audience, and various forms of postings and sharing activities across different formats of SNSs. The current study is considered the first study to take a multidimensional approach to examine the issue of privacy concerns based on every type of posting behavior, ranging from sharing information to one's own network and potentially expanding information to others' networks, and Internet users in general.

Based on the results, implications can be drawn for SNS developers and policy makers.

For SNS developers, it is important to understand where the users' concern for privacy lies for various platforms. Different factors affect privacy concerns on Facebook and Twitter, and other factors may tap into different types of privacy concerns for other SNSs. The results of the current study seem to suggest that users are concerned primarily about being exposed to unwanted audiences for misuse of their personal information. To reduce the concern, if the SNS is not open to providing the data, such as location information for marketing purposes, this should be clearly communicated to the users. For example, the sole purpose of using Foursquare and Swarm is for social check-in; perhaps users could be less concerned about location privacy when using these types of platforms.

The findings of this study also suggest that the overall privacy settings and protections are improved and enforced based on the types of audiences and information being posted. For instance, this study detected that the highest privacy concern on Facebook is what other users are posting to one's timeline. Thus, this study suggests that SNSs should notify users when others post to their timeline, or at least offer a protection function to choose to share or hide such posts. Additionally, Facebook should expand on a user's ability to approve or deny posts that others attempt to display on their timeline. Finally, privacy settings should be expanded based specifically on the two variables outlined in this study, type of posting and type of audience. For Twitter, this study suggests implementing more detailed settings when it comes to who can see one's tweets. Currently, one single unified privacy setting is used for all types of posting options, including to whom one's tweets can be seen. However, Twitter users' primary privacy concern is who can see the tweets they post themselves. Thus, permitting users to grant access to specific audiences to view specific tweets would be beneficial.

The current undertaking also has a couple of implications for policy makers. First, this study suggests that policy makers approach privacy on SNS multidimensionally. As is indicated by the findings of this study, SNS users have different concerns based on posting type and information visible to certain audiences. The privacy policy should be updated to address these concerns. Additionally, privacy policies' visibility and readability should be improved. Past studies have shown that the majority of people do not read privacy policies (Blatterer, 2010). Having a more condensed version of the privacy policy or providing a short summary of its contents will allow readers to understand at least the information that concerns them and have an overall better idea of the information included in the privacy policy.

While we focused on Facebook and Twitter, there are other social networking sites used for various purposes and, thus, users may have different expectations about privacy. For example, Foursquare and Swarm are primarily used to share location information. While the current study found that when other people post a user's location on the user's timeline on Facebook increases privacy concerns regarding marketers, perhaps users would not mind when friends check in the user on Foursquare and Swarm. Snapchat is another example of an SNS that is heavily location-based. Snapchat users often use geofilters created by sponsors of an event or advertisers to communicate the location of their snaps (postings), and thus, privacy concerns may not even arise. In addition, because users may share different types of information on other SNSs, they may experience psychological discomfort towards different types of audiences.

Another limitation of the study is the use of student sample. While the use of SNSs is highest among young adult Internet users, there may be generational differences with regard to privacy concerns on SNSs. For example, a study showed that individuals who are older than 25 believe that their postings would be private unless they make them public. On the contrary, individuals under 25 expect that their SNS postings would be public unless they make them private (Blatterer, 2010). While all SNS users desire to maintain control over who can and cannot access their information, young adults are particularly interested in keeping information private from parents and other authority figures, although they want their information public for their peers and other connections (Blatterer, 2010). Furthermore, many young users perceive that what is considered public on SNS is only public to their network of friends, implying the lack of understanding of public and how their information will be accessed by other users (Blatterer, 2010). Additionally, the participants were heavily skewed toward female SNS users (about 70%). According to Hoy and Milne (2010), female users are generally concerned more about their privacy on Facebook than their male counterparts, particularly for behavioral targeting. Thus, a study with more balanced research participants in terms of age and gender may yield different findings. These limitations should be carefully considered and addressed in future research.

This study has several suggestions for future research. First, as discussed above, extending the current study and employing more generalizable non-student samples, using different types of SNSs, different types of information posting, different posting types, and different types of unwanted audiences will contribute to a more nuanced understanding of privacy on SNSs.

Second, the privacy concern towards marketers is expected to be more significant on SNSs where marketers are allowed to use SNS users' profile and personal information for promotion purposes (Debatin et al., 2009). However, such a concern was not detected in this study. Thus, reexamination of this concern by segmenting SNS promotional activities into several classifications (such as display ads versus native ads and referral ads versus non-referral ads) will provide useful marketing implications on SNSs.

Lastly, future research should include other factors that may influence privacy concerns on SNSs. For example, according to the communication privacy management theory, perceived privacy concern in general is decided by the following factors: intimacy between people (e.g., family, friend, and coworkers) and those who can access the information, the likelihood of public access to the information, control over posted information, trust of the system where the information is shared, and psychological pressure between information withheld and information disclosed (Petronio, 2002). As our study showed, audiences can determine the level of concern for privacy, and while it was not measured in the current study, the level of trust in those who will access the information is found to have a significant impact on privacy concerns (Bergström, 2015). The sensitivity and the perceived use of the information could also have an influence. Chang and Heo (2014) conducted an online survey with young college students and found that the sensitivity of the information is closely associated with the degree of perceived privacy concern on Facebook. In terms of the perceived use of the information, a survey of young German millennials about the adoption of location-based services showed that young users are concerned more about their privacy when their information is used externally than internally (Fodor & Brem, 2015). In addition, digital literacy is another important factor impacting privacy concerns online. Defining privacy literacy as declarative knowledge of technical and legal aspects regarding privacy protection and procedural knowledge of applying protection strategies, Bartsch and Dienlin (2016) found a positive correlation between privacy literacy and privacy protective behaviors. Finally, a survey of adult Internet users showed that technical familiarity, awareness of surveillance technique, and privacy policy knowledge play key roles in privacy control on the Internet (Park, 2013).

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle, & G. Danezis (Eds.), *Proceedings of 6th workshop on privacy enhancing technologies*. Cambridge, UK: PET.

Alloway, T. P., & Alloway, R. G. (2012). The impact of engagement with social networking sites (SNSs) on cognitive skills. *Computers in Human Behavior, 28*(5), 1748–1754. http://dx.doi.org/10.1016/j.chb.2012.04.015.

Altman, I. (1975). *The environment and social Behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Wadsworth Publishing Co.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. http://dx.doi.org/10.1016/j.chb.2015.11.022.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior, 53*, 419–426. http://dx.doi.org/10.1016/j.chb.2015.07.025.

Blatterer, H. (2010). Social networking, privacy, and the pursuit of visibility. In H. Blatterer, P. Johnson, & M. Markus (Eds.), *Modern privacy: Shifting boundaries, new forms* (pp. 73–87). New York, NY: Palgrave Macmillan.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication, 13*(1), 210–230. http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior, 30*, 79–86. http://dx.doi.org/10.1016/j.chb.2013.07.059.

Chen, G. M. (2011). Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others. *Computers in Human Behavior, 27*, 755–762. http://dx.doi.org/10.1016/j.chb.2010.10.023.

Clavio, G., & Kian, T. M. (2010). Uses and gratifications of a retired female athlete's Twitter followers. *International Journal of Sport Communication, 3*(4), 485–500. http://dx.doi.org/10.1123/ijsc.3.4.485.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online Privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x.

Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*, 285–297. http://dx.doi.org/10.1002/ejsp.2049.

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015, January 9). *Social media update 2014. Pew research center*. Retrieved from: http://www.pewinternet.org/2015/01/09/social-media-update-2014/.

Ezumah, B. A. (2013). College students' use of social media: Site preferences, uses and gratifications theory revisited. *International Journal of Business and Social Science, 4*(5), 27–34.

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior, 53*, 344–353. http://dx.doi.org/10.1016/j.chb.2015.06.048.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior, 45*, 168–176. http://

dx.doi.org/10.1016/j.chb.2014.11.083.

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior, 29*(6), 2257–2264. http://dx.doi.org/10.1016/j.chb.2013.05.006.

Hampton, K., Goulet, L., Marlow, C., & Rainei, L. (2012). *Social networking sites and our lives*. Washington, D.C: Pew Research. Retrieved from: http://www.pewinternet.org/Reports/2011/Technology-and-social-networks.aspx.

Hebl, M. R., Williams, M. J., Sundermann, J. M., Kell, H. J., & Davies, P. G. (2012). Selectively friending: Racial stereotypicality and social rejection. *Journal of Experimental Social Psychology, 48*, 1329–1335. http://dx.doi.org/10.1016/j.jesp.2012.05.019.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28–45. http://dx.doi.org/10.1080/15252019.2010.10722168.

Jeong, Y., & Coyle, E. (2014). What are you worrying about on social networking sites? Empirical investigation of young social networking site users' perceived privacy. *Journal of Interactive Advertising, 14*(2), 51–59. http://dx.doi.org/10.1080/15252019.2014.930678.

Johnson, P. R., & Yang, S. (2009). *Uses and gratifications of Twitter: An examination of user motives and satisfaction of Twitter use*. Boston, MA: Presented to Association for Education in Journalism and Mass Communication.

Kim, H.-S. (2016). What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior, 54*, 397–406. http://dx.doi.org/10.1016/j.chb.2015.08.016.

Lipsman, A., Mudd, G., Rich, M., & Bruich, S. (2012). The power of "Like": How brands reach (and influence) fans through social-media marketing. *Journal of Advertising Research, 52*(1), 40–52. http://dx.doi.org/10.2501/JAR-52-1-040-052.

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 9–17). Heidelberg, Germany: Springer.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335–361. http://dx.doi.org/10.1111/j.1083-6101.2007.00328.x.

Mooradian, N. (2009). The importance of privacy revisited. *Ethics & Information Technology, 11*(3), 163–174. http://dx.doi.org/10.1007/s10676-009-9201-2.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. http://dx.doi.org/10.1177/0093650211418338.

Perrin, A. (2015, October 8). *Social media usage: 2005-2015*. Retrieved from: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

Petronio, S. (2002). *Boundaries of privacy: Dialects of disclosure*. Albany, New York: State University of New York Press.

Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology & Behavior, 11*(2), 169–174. http://dx.doi.org/10.1089/cpb.2007.0056.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs, 4*, 323–333.

Roberts, K. K. (2010). Privacy and perceptions: How Facebook advertising affects its users. *The Elon Journal of Undergraduate Research in Communications, 1*(1), 1–11.

Ruggiero, T. E. (2000). Uses and gratifications theory in the 21st century. *Mass Communication & Society, 3*(1), 3–37. http://dx.doi.org/10.1207/S15327825MCS0301_02.

Taddicken, M. (2014). The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248–273. http://dx.doi.org/10.1111/jcc4.12052.

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research, 22*(2), 211–233. http://dx.doi.org/10.1108/10662241211214575.

Thelwall, M. (2011). Privacy and gender in the social web. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 251–265). Berlin Heidelberg: Verlag (Springer).

Urista, M. A., Dong, Q., & Day, K. D. (2009). Explaining why young adults use MySpace and Facebook through uses and gratifications theory. *Human Communication, 12*(2), 216–230.

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(10), 101–115. http://dx.doi.org/10.1111/j.1083-6101.2011.01559.x.

Westin, A. (1967). *Privacy & freedom*. New York: Atheneum.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158–167. http://dx.doi.org/10.1016/j.chb.2014.12.012.