The Privacy Paradox in the Context of Online Social Networking: A Self-Identity Perspective

Philip Fei Wu

Royal Holloway, University of London
Egham Hill, Egham TW20 0EX
United Kingdom

Phone: +44 1784 276287

Email: philip.wu@rhul.ac.uk

# Abstract

Drawing on identity theory and privacy research, this paper argues that the need for self-identity is a key factor affecting people’s privacy behavior in social networking sites. I first unpack the mainstream, autonomy-centric discourse of privacy, and then present a research model that illustrates a possible new theorization of the relationship between self-identity and information privacy. An empirical study with Facebook users confirms the main hypotheses. In particular, the data show that the need for self-identity is positively related to privacy management behaviors, which in turn result in increased self-disclosure in online social networks. I subsequently argue that the so-called “privacy paradox” is not a paradox per se in the context of online social networking; rather, privacy concerns reflect the ideology of an autonomous self, whereas social construction of self-identity explains voluntary self-disclosure.

*Keywords*: self-identity, autonomy, information privacy, privacy paradox, social network sites

The Privacy Paradox in the Context of Online Social Networking: A Self-Identity Perspective

As people leave more digital footprints in this highly connected world, privacy has become “the issue of our times” (Acquisti, Brandimarte, & Loewenstein, 2015, p.509). Information science scholars have been studying people’s privacy perceptions and behaviors in various contexts such as e-commerce (Lowry et al., 2012), e-health (Clarke & Steele, 2015), and online social networking (Wisniewski, Xu, Lipford, & Bello-Ogunu, 2015). A widely adopted conception across different contexts is that privacy means “selective control of access to the self” (Altman, 1975, p. 18). Numerous studies have examined how to protect one’s autonomous self by minimizing the risk of privacy violation by others (Kobsa, Cho, & Knijnenburg, 2016; Smith, Dinev, & Xu, 2011; Vasalou, Oostveen, Bowers, & Beale, 2015).

Although the concept of “self” appears to be central to privacy research, there are surprisingly few studies focusing on the relationship between psychological selfhood and information privacy. While the self is generally defined as a unitary awareness of who one is (Baumeister, 1999), social science scholars have long recognized that social interactions with others contribute a great deal to the formation of self-identity (Jenkins, 2008; Mead, 1967). If the self is indeed an inter-subjective entity being constructed in the presence of others, privacy as a notion of protecting an autonomous self only represents one side of the story. The other side, I contend, lies in the argument that individuals manage their privacy in the process of constructing self-identity through disclosing personal information in social interactions.

Hence, in contrast to the autonomy-protecting view of privacy, I introduce the self-identity concept into privacy research, highlighting the dialectics between one’s *need for self-identity* and his or her self-disclosure behavior. The dialectic relationship between protecting and constructing the self in social interactions suggests new possibilities in theorizing privacy in today’s media-rich information environment. I believe that the need for self-identity provides a theory-informed explanation to the so-called “privacy paradox”, a puzzling phenomenon that people say they are concerned about privacy but act as if they are not (Kokolakis, 2017). I argue that the “privacy paradox” in the context of online social networking might not be a paradox per se; rather, privacy concerns reflect the ideology of an autonomous self, whereas self-disclosure answers the innate need for a socially constructed self-identity.

# Theoretical Background

Social network sites (SNS) such as Facebook build their business models on collecting and monetizing the user data. In order to receive “free” information and communication service, a SNS user must release some of their personal information to the SNS company and advertisers. For example, the user needs to create an account with a verifiable email address and, increasingly, a valid phone number. He or she is often required to provide date of birth, gender, city of residence, and a photo of him/herself. Moreover, the user’s daily activities and personal thoughts shared with friends in the network are visible at least to the SNS platform company. All this personal information will be used to serve commercial purposes such as targeted advertising. As most SNS users are aware of the fact that their personal data are being exploited by commercial entities, the privacy calculus theory contends that people make privacy-related decisions based on weighing the anticipated benefits of the decision against its perceived privacy consequences (Dinev & Hart, 2006; Min & Kim, 2015). Similarly, some researchers draw upon social exchange theory and liken self-disclosure as an exchange of information as goods between individuals and corporates (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

 Hence, privacy in SNS is an art of balancing between autonomy and disclosure, or an act of exchanging bits of “self” for the SNS services. This type of theorization of privacy assumes an existing “true self”. Privacy settings in social information systems, therefore, are designed in such a way that a user’s vulnerable “true self” is shielded from external invasions (Posey, Lowry, Roberts, & Ellis, 2010). The “selective access” conceptualization is in consistent with Altman and Taylor’s (1973) social penetration theory, which likens self as an onion with many layers: The outer layers contain superficial and non-sensitive information that protects an intimate, central core representing the true self. In the progression of social penetration, the protective outer layers are gradually peeled off as one discloses more and more information about oneself in interacting with others. In his later writings, Altman (Altman, Vinsel, & Brown, 1981) moved beyond social penetration theory by emphasizing that social relationships involved both openness and closedness among people. Openness reflects a willingness to expose the self to another person, and closedness means shutting oneself off or withdrawing from others. In this sense, privacy control is a set of mechanisms that regulate interaction with others: people choose how open or closed we are in response to changes in our internal states and external conditions.

But it is possible that people act on a more complex set of mechanisms than the simple trade-off or open-close principle when it comes to privacy. An intriguing observation in some privacy studies is that there is little evidence of correlation between perceived privacy risk and the overall amount of self-disclosure (Taddicken, 2014; Tufekci, 2008). Research has also shown that people can be uncertain about their own privacy preferences even when they are aware of the consequences of their privacy decisions. For instance, in a series of experiments, Brandimarte, Acquisti, and Loewenstein (2013) demonstrated that giving people more control over the publication of their personal information decreases their privacy concerns and increases their willingness to share, even when the risk probabilities remain the same or even increase. To this end, I agree with Nissenbaum’s (2011) view that the “notice-and-consent” (p.34), or “transparency-and-choice” (p.34), approach to addressing privacy issues has failed. Nissenbaum advocates a contextual approach to privacy online, emphasizing the importance of contextual integrity as personal information moves across heterogeneous online contexts. Her theory of contextual integrity offers a critical perspective in analyzing current privacy practices of Internet companies and why those practices are inadequate or misleading. Although not taking a psychological angle, Nissenbaum’s theory points out the urgency of studying privacy as a concept “thickly integrated with social life” (p. 43).

In line with Nissenbaum’s emphasis on social context, my understanding of privacy is rooted in the belief that the self is never “autonomous”. According psychology literature, self-identity is constructed *by oneself and others* about how one is defined and regarded in social life (Jenkins, 2008). Selfhood can be viewed from the perspective of the actor, in which case it refers to how one thinks oneself should be defined and regarded, or from the perspective of others, in which case it refers to how the others define and regard the actor. Identity theorists consider the self as a reflective existence that can categorize itself in relation to other social categories (Stets & Burke, 2000). Through this process of “self-categorization” (a key concept of social identity theory) or “identification” (a key concept of identity theory) [[1]](#footnote-1), self-identity comes into being. Because social categories for each individual vary, identity theorists place a great emphasis on the interconnected individuality in interaction contexts. Therefore, the self does not merely exist at the level of one’s unique individuality (as is usually assumed in autonomy-based view of privacy); rather, the self is always an inter-subjective entity that implies the presence of others. Through a cyclical and negotiating process, individuals come to find self-understanding and be able to express the self-identity (Floridi, 2011).

This socio-psychological understanding of selfhood raises interesting questions about the relationship between privacy and the self. Following the apparent connection between privacy and selfhood, I contend that *the need for self-identity* is an important, but overlooked, factor that could help explain privacy-related inconsistencies and contradictions. Past studies have investigated related concepts such as self-esteem in the context of online privacy. For instance, Schwaig et al. (2013) examined the influence of self-esteem on consumers’ attitude toward information privacy. In their study, self-esteem referred to a person’s belief and feeling of his or her own worth, but the authors considered self-esteem as one of the “individual differences” rather than a more fundamental psychological factor. Xu (2007) applied the concept of self-construal to privacy study and argues that individuals view themselves either as a separate individual (independent self) or as part of a group (interdependent self). Although Xu’s work builds on the notion of self-identity, the two selves were still considered as dichotomous personality and/or cultural traits. James et al. (2016) included self-ego and environment as two separate factors in their interpersonal privacy identity (IPI) model. They rightly point out that privacy involves both information control and social interaction management. Yet, like most other privacy researchers, James et al. hold the view that a “self-ego” independent from environmental influences is the foundation for autonomy and privacy.

In the next section, I adopt a socio-psychological lens of self-identity to investigate how the need for self-identity influences people’s self-disclosure and privacy management in SNS. I propose a set of hypotheses and empirically test a theoretical model to explore possible connections between self-identity and privacy.

# Hypotheses and Research Model

*The need for self-identity* refers to an individual’s need to have a clear sense of self (Schlenker, 1980). The psychological need for self-identity has been well documented in psychology and impression management literature (e.g., Leary, 1996). Most prior studies measure satisfaction of related needs such as self-esteem (Ellison, Steinfield, & Lampe, 2007), or observable behaviors for fulfilling the need for self-identity (e.g., Ma & Agarwal, 2007), rather than the psychological need itself. Drawing on Pierce, Kostova, and Dirks’s (2001, 2003) psychological ownership framework, I decompose the need for self-identity into three aspects: *coming to know the self* (a need to define and learn about the self), *expressing self-identity* (a need to communicate self-identity to others), and *maintaining continuity of self-identity* (a need to maintain an emotional connection between self-identity and one’s past). I postulate that the three aspects of need for self-identity motivate people’s privacy management behaviors. In the context of SNS use, *privacy management* refers to behaviors such as tweaking privacy settings, pruning online personal profiles, and various measures of removing one’s digital footprints (Madden, 2012). I further explain how the three needs relate to privacy management below.

SNS provide people ample opportunities to satisfy their need for self-identity. SNS help define the self through creating user names, choosing avatars, displaying personal interests, and forming social relationships. For example, in creating personal profiles on SNS, individuals contemplate the question – “who am I?” and gather information that represents one’s self-identity. SNS platforms afford various types of feedback (e.g., number of followers, “likes”, comments) that help users see the self through the eyes of others. Hence, an individual *comes to know the self* from contemplating elements that could define his/her self-identity as well as learning about others’ perceptions of his/her self-identity (Min & Kim, 2015).

At the same time, people feel understood and satisfied when their self-presented identities are confirmed in social interactions (Goffman, 1967). The sense of self must be validated and constantly adjusted through *expressing to others*. Evidences of identity expression in online social networks have been documented in the literatures of information science and related fields. Ma and Agarwal (2007) analyzed how technology artifacts in online communities afford identity expression and verification in the process of knowledge sharing. Bumgarner (2007) described Facebook as a place for establishing shared identities through exhibitionism and gossip. boyd and Heer (2006) analyzed millions of Friendster profiles to explore how users express their identities through crafting their profiles. Similar self-presentation and audience management strategies are seen in Twitter networks, where users maintain their self-image through self-censoring their tweets (Marwick & boyd, 2011).

The profiles and posts created in SNS are essentially digital repositories of memories and actions, which helps individual users to *maintain continuity of self-identity* and connect with their past. For example, Facebook Timeline provides the reverse-chronological display of a user's history on Facebook and other life events. A recorded history of one’s past events and actions enables the person to reflect on how the self has been expressed in long-term and therefore helps to construct a coherent sense of self. Moreover, social networking facilitates users’ emotional connection with the self’s past through discovering weak ties and maintaining strong ties (Haythornthwaite, 2002).

Contemplating, expressing, and reflecting on self-identity in the context of social networking require the user to manage privacy options afforded by the SNS platform. From a self-identity perspective, I argue that the very purpose of privacy management is to define the parameters of social comparison (e.g., who can see my profiles and posts), manipulate perceived identity verification (e.g., which side of me should be seen by my friends, co-workers, parents), and therefore satisfy the need for self-identity. Evidences from the literature also support the potential linkage between the need for self-identity and engaging in social media. For instance, Child, Pearson, and Petronio (2009) found that online bloggers with higher levels of internal self-consciousness were more likely to enact blogging privacy management practices. Therefore, I hypothesize that:

**H1**: The need for self-identity is positively related to privacy management activities in SNS.

The need for self-identity is also likely to motivate more self-disclosure of personal information in SNS. It is widely accepted in psychology literature that the sense of self comes into being through the collective experiences of interacting with others (Jenkins, 2008). From this perspective, the three needs of self-identity (need for knowing the self, need for expressing the self, and need for continuity of self-identity) can only be fulfilled through disclosing the self to others. An individual comes to know the self through evaluating implicit and explicit feedback from others on their behaviors, which must be first performed/expressed in the social space. Of course, in order to maintain a coherent self-image in the eyes of others, one needs to continuously release more information about the self over time. Social media researchers have touched upon the connection between self-identity and self-disclosure in their empirical studies. Christofides, Muise, and Desmarais (2009) linked the issue of self-identity to people’s desire for popularity. They postulate that the people who are most popular in SNS are likely to be those whose identity is most actively constructed in social interactions. Therefore, limiting self-disclosure of information in SNS also limits the potential for identity construction and greater popularity. Ellison et al. (2007) described a strong correlation between students’ self-esteem and intensity of Facebook activities among college students. At the same time, SNS companies in general promote the idea of “transparent identity” (van Dijck, 2013, p.200) and encourage users to disclose behavioral data and personal information in the process of socializing. Hence, it is logical to hypothesize:

**H2**. The need for self-identity is positively related to self-disclosure of information in SNS.

When disclosing personal information to satisfy the need for self-identity, SNS users usually picture either a very broad notion of a general audience or more targeted audiences in specific social groups. They rely on privacy management tools to define when to disclose what information with which “imagined audience” (Marwick & boyd, 2011). One would expect that the more a person manages these parameters, the less information the person discloses. The problem is that information often flows across social boundaries and a piece of information intended for a specific social group can find its way into the general audience (Stutzman, Gross, & Acquisti, 2013). As a result, past research shows a much more nuanced reality in terms of how SNS users behave. For instance, in a four-year longitudinal study, Lewis (2011) followed the evolution of privacy behavior on Facebook and discovered an interdependence between friendship decisions and privacy behavior: on one hand, more college students chose to have a private profile over time, although each individual’s network size also increased; on the other hand, students with larger networks are more likely to have a private profile. In other words, there seem to be a strangely positive correlation between the act of keeping things private and the act of making more friends.

These observations corroborate with findings from another stream of privacy research that focused on effectiveness of privacy management mechanisms on SNS platforms. Mondal, Druschel, Gummadi, and Mislove’s (2014) study on social access control lists (SACLs) (e.g., Facebook “Friends Lists” and Google+ “Circles”) reveal the complexity of identifying subsets of friends when sharing. Their findings raise the question about the extent to which those SACLs capture the users’ real privacy preferences. Combining survey and Facebook log data analysis, Bernstein, Bakshy, Burke, and Karrer (2013) discovered that the users’ estimation of their Facebook audience was only 27% of its true size. This mismatch, they argue, might have encouraged more information sharing because some users might not be comfortable broadcasting to a large audience. In Liu, Gummadi, Krishnamurthy, and Mislove’s (2011) sample of Facebook accounts, the privacy settings matched users’ expectations only 37% of the time, and when incorrectly configured, the settings almost always caused more self-disclosure to unexpected audience. These findings lead us to propose:

**H3.** Privacy management activities are positively related to self-disclosure of information in SNS.

Stutzman et al. (2013) provided a plausible explanation for the increased self-disclosure on Facebook: access to increasingly granular privacy settings have increased users’ feeling of control and encouraged high level of self-disclosure. In a series of studies by Xu and her collaborators, the researchers found that privacy management technology and privacy-assurance policies can increase perceived control and subsequently ease people’s privacy concerns (Hoadley, Xu, Lee, & Rosson, 2010; Xu, 2007; Xu, Dinev, Smith, & Hart, 2011). Specifically, they advocate the importance of conceptualizing privacy control as a psychological perception that reflects “an individual’s beliefs in his or her ability to manage the release and dissemination of personal information” (Xu et al., 2011, p. 804). Interestingly enough, in a case study of Facebook News Feed privacy outcry in 2006, Hoadley et al. (2010) acknowledge that the belief that one has control over privacy “may be nothing more than an ‘illusion’” (p.56). The study shows how an “illusory loss of control” triggered users’ perceptions of increasing information accessibility and thus higher privacy concerns, which led to significant changes to privacy management mechanisms by Facebook in response to the outcry. This implies that a proper privacy management mechanism would allow Facebook users to regain a sense of control and be willing to share information again. Hoadley et al. did not empirically test the connection between perceived privacy control and self-disclosure, but I can follow their line of argument by proposing:

**H4**. Privacy management activities have a positive effect on perceived privacy control. The more a SNS user manages his or her privacy settings, the more the user feels in control of privacy.

**H5**. Perceived privacy control has a positive effect on self-disclosure of information. The more a user feels in control of privacy in SNS, the more likely he or she will disclose information.

Like prior studies of online privacy, I also took into consideration some demographic characteristics of SNS users as control variables, including: age, gender, and the intensity of SNS use. These variables may have certain effects on people’s information behavior in SNS ((Ellison et al., 2007; Litt, 2013). The conceptual relationships among the need for self-identity, privacy management, perceived privacy control, and self-disclosure are illustrated in a research model shown in Figure 1.

|  |
| --- |
|  |
| *Figure 1. Research Model* |

# Empirical Study and Results

**Measurement and Pilot Study**

In order to develop a survey instrument to collect data for hypothesis testing, I searched the information science, psychology, and related literatures to identify rigorously validated survey items to measure the constructs specified in the research model. Karahanna, Xu, and Zhang (2015) conducted a literature review on psychological ownership and found no available measurment scales for the needs for self-identity. They then develped a new scale and modeled *the need for self-identity* as a second-order construct with three underlying aspects as its formative first-order constructs. I followed Karahanna et al.’s approach and adapted their scales for measuring the need for knowing the self, the need for expressing the self, and the need for maintaining continuity of self-identity. Each construct is measured by three items (e.g., “I feel a need to discover what kind of person I am.”) and anchored with 1 = strongly disagree and 7 = strongly agree. To gauge *privacy management* behaviors, I used five items from Debatin, Lovejoy, Horn, and Hughes’s (2009) survey of Facebook users’ privacy practices and Madden’s (2012) Pew Internet report on privacy management on social media sites. The scale included statements about common privacy control behaviors across social media platforms, such as adjusting default privacy settings and removing privacy sensitive information in SNS. For online *self-disclosure*, Min (2016) argues that self-presentational information disclosure in SNS is more relevant to user privacy than personally identifiable information disclosure (e.g., name and date of birth). Hence, I adapted survey items from Taddicken’s (2014) Self-Disclosure on the Social Web scale, which assesses the extent to which a person reveals “personal photos”, “personal experiences”, “daily activities”, “thoughts and opinions”, and “feelings, and concerns” in SNS. Lastly, I adapted four *perceived privacy control* measurement items developed by Xu et al. (2011).

I assessed the survey instrumentation’s content validity, construct validity, and reliability. Content validity is usually established through literature review and domain expert review. In this case, all survey items were adapted from previously validated instruments in the literature, and an early version of the questionnaire was sent to three senior academics for review. Additional comments about the questionnaire design were gathered through a free-text question at the end of an online pilot survey (detailed below). After carefully considering both the experts’ and the pilot study respondents’ suggestions, I made minor changes to the instrument, including rephrasing certain items, reordering the blocks of questions, and improving the online interface.

To assess the instrumentation’s construct validity and reliability, I conducted a pilot study with workers on Amazon Mechanical Turk (MTurk). MTurk is an online labor marketplace where registered workers volunteer to perform small tasks. Past research has shown that MTurk has the advantage of reaching a more diversified research population than college students and the quality of data collected on MTurk is as good as that collected in conventional survey environments (Buhrmester, Kwang, & Gosling, 2011). To ensure the quality of the data, I set the prescreening criteria on MTurk to restrict the survey access to workers who had a high task approval rate (greater than 95%), lived in the United States, and were active SNS users. Once a worker accepted the “Human Intelligence Task” or HIT, he or she was then directed to a Web-based survey platform (Qualtrics) where the survey was hosted. Qualtrics was also configured to allow only one survey response from each IP address and the IP must be located in the US. 175 MTurk workers accepted the HIT and 173 responses were complete and usable.

I built a measurement model using SmartPLS and conducted confirmatory factor analysis to assess the validity (convergent validity and discriminant validity) and reliability of the instrument. Convergent validity is the degree to which the measurement items for a theoretical construct are correlated with one another, whereas discriminant validity is the degree to which the measures of each construct differ (Gefen & Straub, 2005). Upon examining the variable loadings and cross-loadings on each construct, I found high variable loadings (greater than 0.70) on their measured construct, with no cross-loadings above 0.40. Reliability is usually assessed by two criteria: Cronbach’s alpha and composite reliability. In this case, Cronbach’s alphas ranged from 0.82 to 0.89 and the composite reliability 0.82 to 0.91, both indicating good reliability of the instrumentation. In summary, the pilot study established the validity and reliability of the construct measures.

**Main Study**

Given the target population of the present study (i.e., active SNS users), I decided to recruit my participants on the most popular SNS platform – Facebook. Conducting the empirical study with Facebook users also helps create a direct dialogue between this study and many previous SNS studies that focused on the same platform. I posted the survey invitation on an American university’s unofficial alumni Facebook Page. The university is a large, public research university located in the East Coast and enrolls more than 37,000 students. The unofficial alumni Page attracted visits from both alumni and some of the current students. At the time I started the survey, the page had accumulated nearly 45,000 “likes” and 139,000 “visits”.

The online survey (hosted on Qualtrics) had been active for approximately two months and I received 274 responses in total. I discarded 25 responses that were either incomplete or had obvious validity issues (for example, identical answers to almost all questions). Therefore, my statistical analysis is based on 249 data points (N = 249). Among the respondents, 137 (55%) were female, 110 (44.2%) male, and two (0.8%) did not reveal their gender. The majority of the respondents were in the age groups of 25-34 (41.8%) and 35-44 (27.7%). This is unsurprising given the fact that most of the visitors to the Page were people graduated from the university in recent years. According to data I extracted from Facebook Insights (facebook.com/ads/audience\_insights) at the time of this writing, the sex distribution in the survey sample is very similar to that of Facebook user population (54% female and 46% male), but I oversampled the 25-44 year olds (Facebook population: 25-34 26% and 35-44 19.5%). Although the sample might not be a representative sample of the Facebook population, I believe it is still a more diverse sample than the college student samples used in previous studies (e.g., Wisniewski et al., 2015).

I examined the validity criteria in SmartPLS to confirm the validity of the measurement model (Table 1). All items loaded higher on their respective constructs than on the other constructs and the cross-loading differences were much higher than the suggested threshold of 0.1 (Gefen & Straub, 2005). The square root of average variance extracted (AVE) for each latent construct is greater than the correlation between the construct and any other construct, which is an important indication of adequate discriminant validity of the measures (Fornell & Larcker, 1981). To test for common method variance (CMV), I followed Craighead, Ketchen, Dunn, and Hult’s (2011) suggestion to use a confirmatory factor analysis (CFA) approach in Harman’s single-factor test. If the covariance among measures is mainly due to common method bias, a one-factor CFA model would fit better than the measurement model. In this case, the one-factor model (*Χ2* =1675.76, CFI =0.49) yielded a considerable worse fit than the measurement model (*Χ2* = 337.45, CFI = 0.94). In addition, I examined the correlation matrix of the factors and found no highly correlated factors (highest *r* = 0.502). Therefore, there is little evidence that common method bias would pose a serious threat to my analysis and interpretation of the data.

| Table 1 *Reliability and Validity of Constructs* |
| --- |
| Constructs | Cronbach’s α | CompositeReliability | AVE |
| *KSLF* | 0.823 | 0.894 | 0.738 |
| *ESLF* | 0.882 | 0.927 | 0.809 |
| *CSLF* | 0.829 | 0.898 | 0.746 |
| *PMGMT* | 0.865 | 0.908 | 0.713 |
| *PCTL*  | 0.874 | 0.914 | 0.727 |
| *SDIS* | 0.925 | 0.941 | 0.728 |

*Note: KSLF = the need for knowing the self; ESLF = the need for expressing the self; CSLF = the need for continuity of self-identity; PMGMT = privacy management; PCTL = perceived privacy control; SDIS = self-disclosure.*

I then examined the structural paths in the research model with all constructs modeled as being reflective, except for the second-order construct of the need for self-identity. I tested the hypotheses by examining the sign and significance of the path coefficients. A bootstrapping technique in SmartPLS was applied to estimate the significance of the path coefficients. Of five hypotheses I assessed, only H5 was not supported by the data. The data analysis results are summarized in Table 2 and illustrated in Figure 2.

| Table 2 *Hypothesis Testing Results* |
| --- |
|  | Path coefficients | *T* value | *P* value | Hypothesissupported? |
| H1: The need for self-identity 🡪 Privacy management (+) | 0.588 | 12.143 | <0.001\*\* |  Yes |
| H2: The need for self-identity 🡪 Self-disclosure (+) | 0.170 | 2.490 | <0.05\* | Yes |
| H3: Privacy management 🡪 Self-disclosure (+) | 0.352 | 5.347 | <0.001\*\*\* | Yes |
| H4: Privacy management 🡪 Perceived privacy control (+) | 0.191 | 2.786 | < 0.01\*\* | Yes |
| H5: Perceived privacy control 🡪 Self-disclosure (+)  | 0.050 | 0.796 | Not significant | No |
| Age 🡪 Self-disclosure | -0.033 | 0.600 | Not significant |  |
| Sex 🡪 Self-disclosure | -0.047 | 0.870 | Not significant |
| Intensity of SNS use 🡪 Self-disclosure | 0.185 | 2.773 | < 0.01\*\* |

|  |
| --- |
|  |
| *Figure 2*. *Model Analysis Results* |

### Discussion of Results

The motivation of this study is to explore a self-identity perspective of privacy in the context of SNS use. My research model presents a possible theorization of the relationships between people’s need for self-identity and their privacy behaviors in SNS. More specifically, the empirical study conducted with Facebook users demonstrates how the need for self-identity is related to behaviors of privacy management and self-disclosure.

The survey data strongly support H1 in that the need for self-identity has a positive effect on people’s privacy management behaviors in SNS (*β* = 0.588, *p* < 0.001). The need for self-identity also explains a significant amount of variance in privacy management (R2 = 0.345). Although the literature on self-identity rarely touches upon the issue of privacy, this result is consistent with psychology research in that individuals high in the need for self-identity are more concerned about what other people think of them and therefore likely to engage in impression management behavior (Reno & Kenny, 1992). In the context of SNS use, the need for self-identity could motivate people to adjust their privacy settings and tidy up their digital breadcrumbs in order to create a more favorable self-image to their intended audience (Min & Kim, 2015). The need for self-identity has a relatively small but statistically significant direct effect on self-disclosure (*β* = 0.170, *p* < 0.05), support H2. The need for self-identity also has an indirect effect on self-disclosure, through privacy management as a mediator. In fact, the positive effect of privacy management on self-disclosure seems strong (*β* = 0.352, *p* < 0.001), indicating that activities such as changing default privacy settings and restricting the readership of their posts could lead to greater degree of information release. This finding corroborates with a small number of previous studies showing that privacy control mechanisms could increase SNS users’ willingness to publish sensitive information (Brandimarte et al., 2013; Stutzman et al., 2013).

Privacy management sets the parameters of one’s boundaries in SNS (i.e., what to show and to whom) and defines one’s initial intention of self-disclosure in social interactions. It is not surprising to see a positive relationship between privacy management and perceived privacy control (*β* = 0.191, *p* < 0.01), thus supporting H4. After all, the very purpose of privacy management is to have some kind of control over one’s privacy. As prior research shows, having the option of adjusting the privacy settings afforded by social networking platforms is likely to give the user a feeling of control (Xu et al., 2011). Brandimarte et al. (2013) believe that this feeling of control gives users a false sense of safety and misplaced confidence, which encourages more self-disclosure. However, the data do not support this postulation in H5. I found no statistically significant relationship between perceived privacy control and self-disclosure. This seems to suggest that Facebook users in the study undertook privacy management in order to feel in control, but this feeling of control had little to do with their actual disclosure of personal information. A possible interpretation of this intriguing finding is that people accept the inevitable consequence of using SNS (i.e., disclosure of personal information), no matter how they feel about privacy control.

Self-disclosure behaviors of the survey participants did not vary systematically by age or gender, but the intensity of SNS use correlated positively with disclosure. This is expected because the more active a user is in SNS the more chances are there for them to disclose information.

In sum, the results support my view that SNS are by definition for co-creating social spaces where individuals fulfill their need for self-identity through managing the self-disclosure. To this end, the common practices among SNS companies that focus on “informed consent” (e.g., lengthy privacy policy agreement) are not in line with why and how users disclose their information (Acquisti et al., 2015). Although individuals attempt to distinguish themselves from their interaction counterparts, the dissimilarities must be expressed and then negotiated in social interactions. SNS users maintain a self-identity that is “simultaneously autonomous and socially valued” (Livingstone, 2008, p. 397). People selectively disclose their information through privacy management in order to construct the self in different social interaction scenarios. A Facebook user could come to know, express, and maintain a professional self-identity in her co-workers network while at the same time present a casual and playful self-image in her close friends circle. The user is likely to disclose different set of personal information within these two social circles, but *the combined amount of information disclosed on the platform is also likely to increase*.

The results also demonstrate that current privacy management mechanisms implemented by many SNS companies do not seem to fit for purpose. SNS platform operators need to respect the fact that different and sometimes conflicting psychological needs co-exist in everyday technology use. While no system design is able to encompass all possible privacy-sensitive social circumstances, an identity-based perspective would encourage system designers to move away from a simple public-versus-private dichotomy. Dourish and Anderson (2006) cite studies of offline information behaviors such as teenagers’ secret-keeping and long-haul truckers’ information behaviors to illustrate that privacy behavior is a marker of social affiliation and group identity. Therefore, privacy could be considered as a collective, rather than individual, information practice (Squicciarini, Xu, & Zhang, 2011).

# Contributions and Implications

This paper critically examines the autonomy-based discourse in information privacy research and argues that the need for self-identity is an overlooked but important factor in understanding people’s privacy behavior. An empirical study of Facebook users confirms my main hypotheses that the need for self-identity relates positively to privacy management and self-disclosure in SNS. I also found that privacy management may boost SNS users’ perceived privacy control, but such perception has little effect on people’s self-disclosure behavior.

The study makes several important contributions. Firstly, my conceptualization of privacy and the empirical results contribute to a deeper understanding of the dialectics in privacy management. I recognize the central role of others in discerning the tension between being public and private, a view in line with Petronio’s (2002) communication privacy management (CPM) theory. CPM highlights the fact that privacy and disclosure are inseparable aspects of a unified dialectical process. Disclosure cannot occur if there exists no private information that can be released to others – “privacy is a necessary condition that one protects or gives up through disclosure” (Petronio, 2002, p. 15). People have to give up some measure of privacy to make the private-public boundary meaningful. However, coming from an interpersonal communication perspective, CPM emphasizes *co-creation of rules* in managing privacy boundaries. By contrast, this paper takes a socio-psychological perspective to explain privacy in relation to the *co-creation of self-identity with others*. In this regard, I expand on the idea of “inherent need to maintain the boundary” (Xu et al., 2011) and provide a self-identity-based explanation for the dialectics in privacy management.

Secondly, this study helps explain the so-called “privacy paradox” in the context of online social interactions, i.e., people say they are concerned about privacy online but act as if they are not. Some researchers have challenged the privacy paradox premise by showing that the more a person is concerned about privacy, the more likely they will employ privacy protection strategies online (Chen, Beaudoin, & Hong, 2016; Utz & Krämer, 2009). These studies tend to focus on SNS users’ profile page protection (e.g., restrict public access to one’s personal profile), rather than a broader range of information activities as investigated in the present study. As I have discussed earlier, fine-grained profile settings may create an illusion of control and actually lead to disclosure of sensitive information to unintended audience in daily communications in SNS (Hoadley et al., 2010). From the perspective of self-identity, it is evident that the seeming “paradox” reveals different innate needs of SNS users. In the process of forming one’s self-identity in social settings, autonomy and disclosure are two sides of the same coin. Individuals are never truly autonomous and privacy is not only about information protection. In a world of mass production and all-pervading commodification, the physical objects we possess are mostly reproducible and identical to what others have. Sociologists believe that anxiety may arise from being unable to discern “self” from “others” in society (Giddens, 1991). This has led to, in the words of Floridi (2010), rampant “informational re-appropriation” (p.15) in online spaces: We try to retain individualism by giving away individual details. In other words, *we share information about ourselves to become less informationally indiscernible*.

Thirdly, this study supports the view that SNS platform designers should adopt privacy management approaches that go “beyond access control” (Mondal et al., 2014, p.1). The tick-box approach makes sense in relatively straightforward transactional relationship between consumers and merchants, but fails to capture the fluidity and complexity of social identity. The one-size-fits-all privacy settings may result in what Marwick and boyd (2011) have termed “context collapse”, where privacy-sensitive contexts are not distinguished in access control mechanisms. Individual users are either forced to perform for the lowest common denominator of the broadest possible audience, or struggle to produce plysemic selves that are inherently consistent (Papacharissi & Gibson, 2011). Some SNS platforms have begun to recognize the privacy needs in different scenarios and tweaked their platform designs in recent years. For example, Google+ Circles and Facebook Groups allow users to categorize their connections based on social categories (acquaintances, close friends, co-workers, etc.). An individual’s privacy valuation in each of these circles or groups would be different. Such changes are encouraging, but still not fully addressing the fluidity of social circles and dynamics of self-identity formation. In academic research, Squicciarini, Xu, and Zhang’s (2011) idea of collaborative privacy management in online social networks is a step closer to identity-based privacy management. Similarly, Lampinen, Lehtinen, Lehmuskallio, and Tamminen (2011) proposed a design framework that considers disclosure as an interpersonal process in which people collaboratively choose what to disclose about each other.

Finally, conceiving privacy in relation to self-identity helps avoid pitfalls in “normative and sometimes emotionally charged” privacy debates (Smith et al., 2011, p. 1003). Autonomy is a value-laden term that carries the baggage of liberal individualism (Cohen, 2012), which may overshadow alternative conceptualizations of privacy in academic discussions. Identity, on the other hand, is a more neutral concept that has been included in diverse discourses in various intellectual traditions. An identity-based privacy view may help encourage diverse theorizations and new insights in privacy research.

# Limitations and Future Research

It is worth clarifying that I am not arguing for the superiority of the self-identity perspective over other frameworks in studying information privacy, nor do I imply that the research model presents a complete picture of complex relations between self-identity and other socio-psychological factors relevant to privacy. Rather, my aim has been to illustrate the potential of a somewhat overlooked concept in explaining SNS users’ privacy behavior and in generating plausible and interesting hypotheses. To this end, this study has its limitations and leaves some open questions for future research.

First, the study focuses on self-identity of individual users in a large SNS with heterogeneous social relationships, omitting the important dimension of group identity in small social groups with more homogeneous social relationships (Squicciarini et al., 2011). Social psychologists and information science researchers have long observed the effects of group identity on individual members’ behavior, both offline and online (e.g., Ahn, 2011; Terry, Hogg, & White, 1999). According to Smith et al.’s (2011) interdisciplinary literature review, very few studies have considered the group level of analysis in information privacy research. Several promising research questions arise when consider both identity and privacy at a group level: In an online social group, how does an individual’s self-identity interact with her group identity in shaping her privacy behavior? Does a strong identification with the group lead to more disclosure of personal information? If there is not a clear-cut public/private boundary in self-identity formation, are SNS platforms responsible for shaping “zones of privacy” (Fahey, 1995, p. 688) through social categorization and norms? Future work could be carried out to investigate how norms and collective identity influence both individual and group privacy behaviors (Bloustein, 1978) in a particular social group in SNS.

Second, my theorization and the research design center on the specific context of online social networking, where the active construction of self-identity occurs in social interactions. The self-identity perspective is less applicable to non-social contexts such as e-health and e-commerce, where the privacy concern is mostly about unwanted access to personally identifiable information (Clarke & Steele, 2015; Lowry et al., 2012). On the other hand, SNS platforms are also evolving toward more fine-grained privacy management settings due to people’s increasing privacy awareness and the stricter data protection policies imposed by government. This developing landscape of privacy management invites further research on the linkage between identity theories and privacy behavior, taking into account user-system dynamics, platform differences, and the changing sociocultural environment.

# References

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

Ahn, J. (2011). The effect of social network sites on adolescents’ social and academic development: Current theories and controversies. *Journal of the American Society for Information Science and Technology*, *62*(8), 1435–1445.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Monterey, California: Brooks/Cole Publishing Company.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships.* New York: Holt, Rinehart, and Winston.

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Psychology*, *14*, 107–160.

Baumeister, R. F. (1999). *The self in social psychology*. Psychology Press.

Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 21–30). New York, NY, USA: ACM.

Bloustein, E. J. (1978). *Individual and group privacy*. New Jersey: Transaction Books.

boyd, danah, & Heer, J. (2006). Profiles as conversation: Networked identity performance on Friendster. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS ’06)*. Kauai, HI.

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

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*(1), 3–5.

Bumgarner, B. A. (2007). You have been poked: Exploring the uses and gratifications of Facebook among emerging adults. *First Monday*, *12*(11).

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology*, *67*(12), 2871–2881.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, *60*(10), 2079–2094.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341–345.

Clarke, A., & Steele, R. (2015). Smartphone-based public health information systems: Anonymity, privacy and intervention. *Journal of the Association for Information Science and Technology*, *66*(12), 2596–2608.

Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven, CT: Yale University Press.

Craighead, C. W., Ketchen, D. J., Dunn, K. S., & Hult, G. T. M. (2011). Addressing common method variance: Guidelines for survey research on information technology, operations, and supply chain management. *IEEE Transactions on Engineering Management*, *58*(3), 578–588.

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.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human Computer Interaction*, *21*(3), 319–342.

Ellison, N. B., Steinfield, C., & 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.

Fahey, T. (1995). Privacy and the family: conceptual and empirical reflections. *Sociology*, *29*(4), 687–702.

Floridi, L. (2010). *Information: A very short introduction*. Oxford, UK: Oxford University Press.

Floridi, L. (2011). The informational nature of personal identity. *Minds and Machines*, *21*(4), 549–566.

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

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1). Ret

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Redwood City, CA: Stanford University Press.

Goffman, E. (1967). *Interaction ritual: Essays on face-to-face interaction*. Oxford, UK: Aldine.

Haythornthwaite, C. (2002). Strong, weak, and latent ties and the impact of new media. *The Information Society*, *18*(5), 385–401.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60.

Hogg, M. A., Terry, D. J., & White, K. M. (1995). A tale of two theories: A critical comparison of identity theory with social identity theory. *Social Psychology Quarterly*, *58*(4), 255–269.

James, T. L., Nottingham, Q., Collignon, S. E., Warkentin, M., & Ziegelmayer, J. L. (2016). The interpersonal privacy identity (IPI): Development of a privacy as control model. *Information Technology and Management*, *17*(4), 341–360.

Jenkins, R. (2008). *Social identity* (3 edition). London & New York: Routledge.

Joinson, A. N. (2008). Looking at, looking up or keeping up with people? Motives and use of Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI’08)* (pp. 1027–1036). New York, NY, USA: ACM.

Karahanna, E., Xu, S. X., & Zhang, N. (Andy). (2015). Psychological ownership motivation and use of social media. *Journal of Marketing Theory and Practice*, *23*(2), 185–207.

Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology*, *67*(11), 2587–2606.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

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

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). We’re in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3217–3226). New York, NY, USA: ACM.

Leary, M. R. (1996). *Self-presentation: Impression management and interpersonal behavior*. Boulder, CO: Westview Press.

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 91–109). Berlin Heidelberg: Springer.

Litt, E. (2013). Understanding social network site users’ privacy tool use. *Computers in Human Behavior*, *29*(4), 1649–1656.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 61–70). New York, NY, USA: ACM.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers’ use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393–411.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, *63*(4), 755–776.

Ma, M., & Agarwal, R. (2007). Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities. *Information Systems Research*, *18*(1), 42–67.

Madden, M. (2012). *Privacy management on social media sites*. Pew Research Center. Retrieved from http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

Marwick, A. E., & boyd, danah. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133.

Mead, G. H. (1967). *Mind, self, and society: from the standpoint of a social behaviorist*. Chicago: University of Chicago Press.

Min, J. (2016). Personal information concerns and provision in social network sites: Interplay between secure preservation and true presentation. *Journal of the Association for Information Science and Technology*, *67*(1), 26–42.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, *66*(4), 839–857.

Mondal, M., Druschel, P., Gummadi, K., & Mislove, A. (2014). Beyond access control: Managing online privacy via exposure. In *Proceedings of the Workshop on Usable Security (USEC ’14)*. San Diego, CA, USA.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–90). Heidelberg: Springer.

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

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *Academy of Management Review*, *26*(2), 298–310.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology*, *7*(1), 84–107.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems*, *19*(2), 181–195. h

Reno, R. R., & Kenny, D. A. (1992). Effects of self-consciousness and social anxiety on self-disclosure among unacquainted individuals: An application of the social relations model. *Journal of Personality*, *60*(1), 79–94.

Schlenker, B. R. (1980). *Impression management: The self-concept, social identity, and interpersonal relations*. Brooks/Cole Publishing Company.

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers’ perceptions of the invasion of information privacy. *Information & Management*, *50*(1), 1–12.

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

Squicciarini, A. C., Xu, H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology*, *62*(3), 521–534.

Stets, J. E., & Burke, P. J. (2000). Identity theory and social identity theory. *Social Psychology Quarterly*, *63*(3), 224–237.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41.

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.

Terry, D. J., Hogg, M. A., & White, K. M. (1999). The theory of planned behaviour: Self-identity, social identity and group norms. *British Journal of Social Psychology*, *38*(3), 225–244.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36.

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2).

van Dijck, J. (2013). ‘You have one identity’: performing the self on Facebook and LinkedIn. *Media, Culture & Society*, *35*(2), 199–215.

Vasalou, A., Oostveen, A.-M., Bowers, C., & Beale, R. (2015). Understanding engagement with the privacy domain through design research. *Journal of the Association for Information Science and Technology*, *66*(6), 1263–1273.

Wisniewski, P., Xu, H., Lipford, H., & Bello-Ogunu, E. (2015). Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology*, *66*(9), 1883–1896.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. In *Proceedings of 28th Annual International Conference on Information Systems (ICIS 2007)*. Montréal, Canada.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12).

1. Identity theory and social identity theory have roots in different intellectual traditions, yet these two theories have substantial overlap. See Hogg et al. (1995) and Stets and Burke (2000). [↑](#footnote-ref-1)