

An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies

Wannes Heirman, Michel Walrave, Anne Vermeulen, Koen Ponnet, Heidi Vandebosch, Joris Van Ouytsel and Ellen Van Gool

Department of Communication Studies, University of Antwerp, Antwerp, Belgium

ABSTRACT

Users of social network sites (SNSs) use three main strategies that help to manage the privacy of their profile information: (1) *limiting the level of data revealed*, (2) *using privacy settings* to exert control over data and (3) *audience/friendship management* by being restrictive about whom to accept as a 'friend'. Extant research does not show whether these strategies operate as independent mechanisms or whether they are interdependent and work as a *system*. Given what offline privacy theorist Irwin Altman (1977) designates as the *multi-mechanic nature* of privacy protection, we test a model in which we expect to find that the three discerned strategies are related to one another. Structural equation modelling analysis performed on the subsample ($n = 1564$) of our study's data – collected among 1743 adolescents by means of a paper-and-pencil survey – demonstrates that, in line with Altman's vision of privacy protection, the three discerned strategies effectively operate as an interdependent system. In congruence with the hypotheses derived from extant research, we found that adolescents' level of disclosure influences adolescents' involvement in the two other discerned strategies: Adolescents with high levels of personal information disclosure share an increased tendency to have many friends on SNSs and a lower level of using privacy settings.

ARTICLE HISTORY

Received 8 July 2015
Accepted 12 April 2016

KEYWORDS

Adolescents; ICT; disclosure; privacy settings; SNS audience

1. Introduction: information privacy on social network sites

The majority of people living in Western societies have rapidly embraced social network sites (SNSs) as a part of their daily lives (WIP 2013). This evolution is said to have changed the nature of social relationships (Wilson, Gosling, and Graham 2012). People belonging to different social contexts (e.g. family, work and friends) are now unified in one network of SNS friends (Ellison, Steinfield, and Lampe 2007). An individual's profile can be considered as an online stage where people can, besides communicating with other contacts belonging to their friends list, also present themselves towards others by revealing personal information (Siibak 2009).

Several studies have demonstrated that SNSs have the potential to fulfil adolescents' developmental needs such as identity formation and interaction with friends (Boyd 2008; Ellison, Steinfield, and Lampe 2007). Research has yielded a positive association between revealing personal information online and users' level of self-identity and general well-being (e.g. Pelling and White 2009). SNS use may also help to reconsolidate previous relationships and to pursue relationships with people only briefly or occasionally met in an offline context (Ellison, Steinfield,

and Lampe 2007). In this way, SNSs enable people to maintain (or as Putnam (2000) formulates it: to *bond*) and to increase (to *bridge*) social capital. Extensive evidence is available in the literature for the beneficial effects of high levels of social capital (for an overview, see Lin, Cook, and Burt 2008).

The way in which SNS providers encourage users to disclose as much information as possible has, however, also attracted a lot of criticism and concerns on behalf of policy-makers, educators and parents. One of the issues that emerges most on the forefront of the public debate regarding SNSs is that of privacy and how to adequately protect the information shared by an ever-growing crowd of SNS users (Young and Quan-Haase 2009). Moreover, empirical evidence suggests that many children younger than 13 have already made their own profile on SNSs, easily enabled by circumventing age restrictions and lying about their age. For instance, according to the EU Kids Online data collected among approximately 25,142 European 9–16-year olds, 26% of children aged 9 or 10 years old have their own profile, whereas most providers based on the Safer Social Networking Principles (in the European Union) and other legal ramifications (e.g. the Children's Online

Privacy Protection Act (COPPA) in the USA) install a minimum age of 12 or 13 years as a requirement to use their services (Livingstone et al. 2011).

Concerns related to privacy on SNSs can partially be explained by the affordances of digital content (Boyd 2008; Papacharissi and Gibson 2011): the *persistence*, *scalability*, *replicability*, *searchability* and *shareability* of digital content. The notion of online persistence refers to the adage 'what appears online stays online' (Debatin 2011). This entails that due to the easy storage possibilities of digital media, people can be linked for their further lives with information online that possibly disreputes them (e.g. when pictures at a party are consulted by the employer of this person). According to an American study (Madden et al. 2012), parents report being very concerned that the information provided online by their children may have implications for their reputation and employment chances in later life. A second affordance of digital content is that, once posted online, it can virally spread itself across the web. Put otherwise, a digital message is easily scalable from one recipient to a vast audience. Moreover, it is very easy to replicate digital data. Also, the excerpts of an intimate chat conversation can easily be copy-pasted into another online venue with more visibility (e.g. the 'wall' of a fake profile), which clearly shows how this affordance has an impact on users' privacy. Another affordance of digital content that poses a potential threat to users' privacy is that profiles can easily be searched using keywords. A fifth affordance that has the potential to impact users' privacy is the shareability of digital content. In theory, all interactions through SNSs leave digital footprints, and due to the inherent *bit-based* nature of SNSs, these traces can be shared among the members of a vast online audience. Several parties are interested in personal data available on social media, such as in the first instance online marketers (Pekárek and Leenes 2009). Evidence also exists about employers scrutinising job candidates' Facebook profiles to assess their candidacy (Hoek, O'Kane, and McCracken 2016) and public courts basing their verdict on what is revealed on social media (Russon 2015).

Some studies have focused on the psychological risks such as feeling anxious, embarrassment and regret after disclosing more or less sensitive data on SNSs (e.g. Christofides, Muise, and Desmarais 2012). Another psychological discomfort associated with the disclosure of information on SNSs is the tension it possibly creates across the different social spheres in which an SNS user is embedded. A specific user's friends list on SNSs is featured by a high degree of heterogeneity, with contacts belonging to diverse social contexts. Comments posted by people belonging to one social sphere (e.g. friends at the sports club) can also be read by 'outsiders' (e.g. family

members). In this way, some information shared on SNSs may be entirely appropriate for the profile owner's real-life friends, whereas contacts from other contexts may feel negatively about the posting of such content (e.g. older family members or colleagues/superiors). Such tension between *friend contexts* is relatively less an issue in the offline environment, where different groups are partitioned in different contexts that are physically delineable and not merged like in an SNS friends list (Marwick and Boyd 2011). Research has shown that users are aware of this potential *online conflict* of social contexts. Such awareness can create a certain degree of tension, which is related to the difficulty of determining which information is appropriate to share across all social spheres simultaneously (Lampinen, Tamminen, and Oulasvirta 2009). Some authors (e.g. Marwick and Boyd 2011) anticipate that this tension may urge some users to limit their disclosure on SNSs to the lowest common denominator by only posting content that can in no way be interpreted as offensive by any of the contacts included. Other scholars (e.g. Oolo and Siibak 2013) argue that SNS users, especially younger adolescents, experience difficulties in imagining the audience they have created for their profile uploads by accepting friends on SNSs.

Another privacy-related risk is that the digital traces left by SNS users are being processed and analysed by providers for commercial purposes. Scholars have observed an inclination among SNS providers to keep information as public as legally possible by default, because an SNS 'is only as good as the content that users share' (Wilson, Gosling, and Graham 2012, 212). The amount of data shared on SNSs directly determines the economic taxation of an SNS provider. Each piece of personal data disclosed on SNSs helps the provider learn more about its users. The latter can pass on this knowledge to companies interested in reaching a specific segment of consumers with highly targeted communication. Moreover, as Pekárek and Leenes (2009, 3) argue, 'this process is cyclically reinforced: the more information people leave on the SNS, the richer the profiles become, the more attractive they are for both commercial use and social use by other (potential) SNS members'.

The worrying about users' privacy on SNSs has not gone unheard. Besides the implementation of policy initiatives (e.g. Safer Social Networking Principles for the European Union), the extent to which the content of a profile is visible arises from several choices that SNS users make as they construct and manage their online networks (Madden et al. 2013).

1.1. Privacy-protective strategies

In this context, current privacy literature discerns three strategies by which users can manage the privacy of

their profile on SNSs (Ellison et al. 2011; Wilson, Gosling, and Graham 2012): (1) limiting one's level of disclosure on SNSs (in other words, *disclosure management*), (2) *controlling* the disclosed information by applying *privacy settings* and (3) managing the size of the audience able to consult the disclosed information (in other words, *audience/friendship management*).

1.1.1. Privacy-protective strategy 1: disclosure management

The first way in which a user can help protect personal information on SNSs is by not engaging in extensive disclosure within these platforms (Debatin et al. 2009; Madden et al. 2013; Young and Quan-Haase 2009). From the perspective of enhancing information privacy, it is better to carefully consider the appropriateness of each bit of information disclosed online, instead of freely divulging information without restraint. In the context of SNSs, self-disclosure has been defined as 'the amount of information shared on a user's profile as well as in the process of communication with others' (Krasnova and Veltri 2010, 1). Research has revealed that many SNS users less likely disclose specific information if they anticipate that the content of this disclosure could be problematic in some way or another (Lampinen, Tamminen, and Oulasvirta 2009; Young and Quan-Haase 2009). This implies that in such cases users deliberately perform self-censorship in order to warrant their privacy.

1.1.2. Privacy-protective strategy 2: control by privacy settings

If users decide to disclose information on SNSs, the question emerges of what level of protection should be applied to the uploaded content. Privacy settings offer users a control mechanism to determine their desired level of protection by limiting the access to a specific piece of their data, ranging from a broad audience (*everyone*) to a narrower group of users (e.g. *friends of friends*, *only friends* or *restricted to myself*) (Stutzman and Kramer-Duffield 2010; Young and Quan-Haase 2009). Moreover, since the year 2009, the world's largest SNS provider, Facebook, allows users to determine the level of access to nearly each piece of content. Displayed next to each disclosed item on their wall, there is an icon that allows users to choose with whom they want to share the particular piece of content. In this way, it is possible to give access to a specific photo, except for some specific contacts (e.g. parents or colleagues) in one's friends list. In short, these customised privacy settings enable SNS users to differentiate the level of access to one's data between people listed as friends on their profile. Hereby, it becomes possible for profile owners to divide their SNS platform into separate spaces of

privacy (Young and Quan-Haase 2009). The existence of privacy settings is important as it appears that teens with fully public profiles are more likely to have bad experiences on these platforms than teenagers with a fully private profile (23% vs. 12%) (Lenhart et al. 2011).

1.1.3. Privacy-protective strategy 3: friendship/audience management

Privacy settings alone, however, do not suffice for individuals to protect themselves and their personal information from privacy infringements on SNSs. These settings have been criticised precisely because privacy advocates argue that they create a false feeling of privacy and security (Debatin 2011; Madden et al. 2013). As posited by Madden et al. (2013), the size and composition of an individual's friend network have a great bearing on how private a *friends-only* setting can be. Therefore, as a third strategy of managing the privacy of their profiles, users can also limit the audience witnessing their personal information by being more restrictive in whom to accept as friends on SNSs (Debatin et al. 2009; Madden et al. 2013; Young and Quan-Haase 2013). Admitting unknown people to one's friends list implies that these latter have full access (unless configured otherwise) to the information contained in the profile of the person granting the friend request.

To our knowledge, few, if any, studies have to date integrated the three discerned strategies into one research model and subsequently ran analyses to test the fit of the entire model. Empirical studies to date mostly run analyses (usually regressions) for each privacy-protective strategy separately. For instance, the study by Christofides, Muise, and Desmarais (2009) examines which factors help to predict information disclosure and privacy setting use by conducting two separate regression analyses. Similarly, Spiekermann et al. (2010) examine the predictors of information disclosure on Facebook, without taking any other strategy into consideration in testing their research model. This study will take a different angle that enables us to examine whether the three discerned strategies work as independent or interdependent mechanisms for the privacy of adolescents' information on SNSs. Doing so, we will base ourselves on Irwin Altman's privacy theory and the findings of other extant research.

Two reasons can be discerned for why this article specifically focusses on adolescents. First, a systematic literature review reveals that whilst being the most prevalent form of online risks among adolescents (Hasebrink, Livingstone, and Haddon 2008), the risks associated with young people's online privacy remain the most understudied when compared to other online risks with which young people are confronted (Slavtcheva-Petkova,

Bulger, and Nash 2013). By focusing on this young group of Internet users, this study hereby clearly contributes to a clear gap in the literature. Second, the notion of privacy is of great importance for adolescents. As argued by several scholars (e.g. Peter and Valkenburg 2011), in no other life stage does privacy play such a critical role as during adolescence. Weinstein, Simon, and David (1987) explain this by arguing that privacy constitutes one of the crucial conditions for a satisfactory childhood environment, as it fosters the development of personal *identity*, encourages the growth of *competence* and promotes a sense of *security* and *trust*. There is a clear link between these functions of privacy and the developmental goals of adolescence (Peter and Valkenburg 2011). Moreover, additional research has revealed that privacy fosters the learning of crucial *skills* needed to achieve these developmental goals (Buhrmester and Prager 1995; Peter and Valkenburg 2011). In other words, online privacy is highly relevant to adolescents' development and well-being, hence the present study's focus on this younger age segment.

The main objective of this study is to test whether Irwin Altman's theory, which dates back to the pre-Internet era, is also applicable to the way adolescents regulate their privacy on SNSs by adopting a multitude of privacy-protective strategies that work as a 'system'. This results in our main research question: Is there a relation between these three strategies or do they work independently from one another? Subsequently, as an additional aim of this research and based on the extant literature (see section 2), we want to test whether disclosure management acts as a predictive strategy of the two other mentioned privacy-protective strategies: so, does disclosure management predict online audience management and the use of privacy settings?

1.2. Altman's multi-mechanic privacy theory

According to Altman (1977, 67), 'privacy is viewed as involving a network of behavioral mechanisms that people use to achieve their desired levels of social interaction'. One of Altman's key ideas was that people mostly adopt a mix of privacy-protective behavioural mechanisms that operate as an interdependent system, rather than operating independently and separately (Altman 1977, 67): 'As such, they include properties of interdependence and of compensatory and substitutable action. That is, a person may use different mixes of behaviors to achieve a desired level of privacy'. Our study aims to investigate whether Altman's idea of privacy-regulating mechanisms working as a system also applies to the online environment and more specifically to SNSs. In addition, we have integrated additional constructs in the

model that we expect may partially drive adolescents' use of the three discerned privacy-protective strategies. The rationale for their inclusion in the model is further explained in the next paragraphs, but these additional variables are need for popularity (NFP; see Section 2.1), the motivation to meet new people (see Section 2.2) and profile page experience (see Section 2.3).

2. Hypotheses development

We derive five hypotheses from the literature (see Figure 1). In the following section, we elaborate on how we inferred the hypotheses for the present study.

2.1. Need for popularity

Adolescence is a life period during which teenagers start to develop a better sense of who they are and with whom they belong (Steinberg 2011). In no other age group does the development of identity take such a central place as within this life phase. This can partially be explained by the observation that during adolescence teenagers start to develop a wider range of relationships with peers (Rotenberg 2006). Peers give each other feedback, which is acknowledged in the literature as one of the key catalysts for youngsters' identity development (Buhrmester and Prager 1995; Steinberg 2011). In both online and offline environments, adolescents are receiving inputs from others about whom they are or how they are perceived. Moreover, during these interactions, they receive feedback about whether these attributes are being appraised or not. In this context, it may well be that SNSs such as Facebook may increase the importance of popularity due to the public nature of other peers' friends lists, their disclosures and the positive or negative feedback they receive (Utz, Tanis, and Vermeulen 2012). Moreover, most SNSs offer individuals specific affordances that may be especially important for individuals who are sensitive to popularity (Christofides, Muise, and Desmarais 2009). For instance, users can engage in social browsing to make new acquaintances in order to expand their SNS friends list and, in doing so, add to their perceived popularity. Also, the fact that the total number of friendships of a specific user is displayed (a number that is by default accessible for all users, even those not friended) may entice adolescents who desire to be popular among peers to be even more motivated to use SNSs to broaden their social circle by making new friends online. In sum, it is plausible that users characterised by a higher NFP will be more inclined to use SNSs to meet new people (Utz, Tanis, and Vermeulen 2012). Therefore, the following is expected:

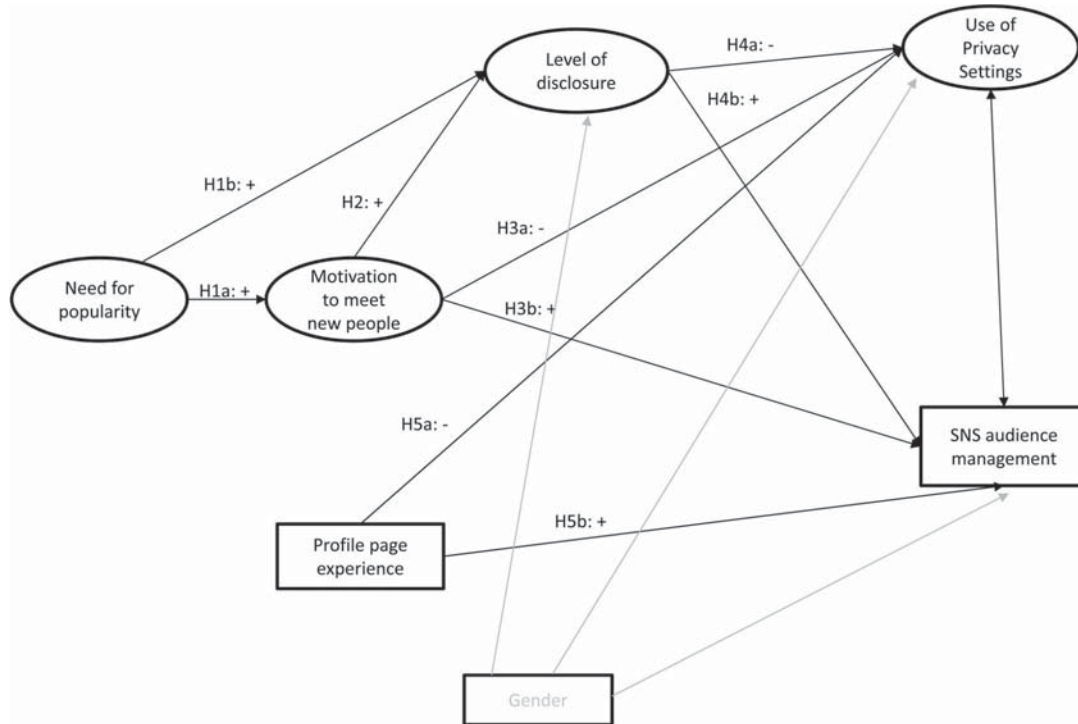


Figure 1. Proposed model.

H1a: The more adolescents feel the need to be popular, the more they will be inclined to use SNSs for meeting new people.

H1b: The more adolescents feel the need to be popular, the higher the level of disclosure on their profiles.

As shown in previous research, SNSs are online platforms that allow users to selectively present themselves and, to a certain extent, manage the impression other users are forming about them (Ong et al. 2011; Siibak 2009; Utz, Tanis, and Vermeulen 2012). Especially the asynchronous nature (users have time to reflect on what they post) and controllable nature (users can edit their posts even after being uploaded) of most communication on SNSs allow individual adolescents to project an ideal image of themselves on their profiles (Debatin et al. 2009; Mesch and Beker 2010). Some studies have associated people's motivation to be popular with their levels of online self-disclosure; One previous study revealed a positive relationship between respondents' NFP and their level of disclosure on SNSs (Christofides, Muise, and Desmarais 2009), whereas another study established a relation between the disclosure of feelings on SNSs and the uploading or editing of pictures (Utz, Tanis, and Vermeulen 2012). By adding personal information, uploading pictures and posting regular status updates, adolescents can augment the chances of receiving feedback (Valkenburg, Peter, and Schouten 2006). The insights generated by previous studies give rise to the following hypothesis:

2.2. The motivation to meet new people

Previous studies have found an association between users' motivation to use SNSs for social seeking purposes and the extent to which they disclose information on their profiles (Chang and Heo 2014; Ellison et al. 2011). This is not entirely surprising as profiles containing much information about the profile owner will generate more interest and trust among other users potentially interested in becoming SNS friends. Moreover, regularly disclosing personal information on SNSs (e.g. by posting status updates, pictures or videos) can increase the visibility of the profile owner, unless privacy settings are configured otherwise, not only among friends but also *friends of friends*. In this way, with each new item of personal information, a profile owner augments his chance of being noticed by others (mainly friends of friends) and to create common ground and connect with others. Doing so allows adolescents to extend their friends list and also to elicit additional feedback from others (Valkenburg, Peter, and Schouten 2006). Therefore, we expect that:

H2: The more adolescents show a tendency to use their profile page with the purpose of meeting new people, the

more frequently they will disclose personal information on their profile.

Essentially, privacy settings allow SNS users to (a) restrict the information contained in their profile to a specified set of people (*friends, friends of friends, customised privacy settings* or *everyone*) and (b) hide one's profile for people who are not listed as *friends* or *friends of friends* (or customised settings allowing specific SNS-friends access, while denying access to other specific people listed as friends on SNSs) (Ellison, Steinfield, and Lampe 2007; Ellison, Steinfield, and Lampe 2011; Young and Quan-Haase 2013). The use of privacy settings, however, can be counterproductive in case the profile owner mainly uses his/her profile to get acquainted with new people, as strict privacy settings entail that their profile will be difficult or impossible to retrieve for those not belonging to their network of friends. It is found that adolescent users interested in meeting new people on SNSs take a more permissive approach to handling their privacy settings (Walrave, Vanwesenbeeck, and Heirman 2012). A study conducted by Stutzman and Kramer-Duffield (2010), however, found a positive relation between network size and having a profile page set to *friends only*. The authors of this latter study explain this finding by alluding to the existence of a point of *saturation* in increasing the size of one's list of friends on SNSs. This may be because the individual feels he or she has enough friends or that nearly all desired contacts are already present in the friends list. In such a context, a profile owner may no longer feel the need to connect with additional people on SNSs, may feel the gain of having an open profile is too small and, therefore, may set his or her profile to private (Stutzman and Kramer-Duffield 2010). Although previous studies have painted a mixed picture, we expect the following:

H3a: There is a negative association between adolescents' motivation to use SNSs with the purpose of meeting new people and the extent to which they use privacy settings to shield their data on SNSs.

Previous Korean research established a positive association between motivations to use SNSs for social investigation purposes (e.g. to meet new people and to search for new contacts) and the number of friends one has on a profile page (Jang Hyun, Min-Sun, and Yoonjae 2010; Kim, Sohn, and Choi 2011). More specifically, it was found that students with a higher need to seek new friends on SNSs tend to have the largest friend networks. Moreover, this psychological need for connecting with other people online was found to be a strong significant predictor of the number of friends adolescents had on their profile page (Jang Hyun, Min-Sun, and Yoonjae

2010; Kim, Sohn, and Choi 2011). Given the latter studies, we expect:

H3b: There is a positive association between adolescents' use of SNSs to meet new people and the number of friends in their online contact list.

An American study reveals that most people using privacy settings disclose less information than those who do not actively manage their profiles in this way (Young and Quan-Haase 2009). This result conflicts with an investigation by Christofides, Muise, and Desmarais (2010), which found that the likelihood of adopting privacy settings was not related to the likelihood of disclosing information on Facebook. Christofides, Muise, and Desmarais (2010, 13) themselves were surprised with this result as they argued that 'based on traditional privacy literature, it would be expected that those who desire more control over their information would engage in less disclosure'. Notwithstanding the mixed results of early research, this study derives its hypothesis from Young and Quan-Haase (2009) and thus expects that people who are sensitive to privacy will not only disclose less personal information, but also exert higher control over the information they decide to disclose.

H4a: There is a negative association between adolescents' level of disclosing information on SNSs and the extent to which they protect their information on these platforms by using privacy settings.

The most recent Pew study on teens and social media revealed that teens' sharing of a large amount of social capital on SNSs includes a greater variety of contacts (in terms of background) as friends in their profiles (Madden et al. 2013). Also, they tend to share a wider variety of personal information on these platforms. In this regard, the study demonstrated that teens with an above-average network size were more likely to include specific pieces of personal information (e.g. a true photo of themselves, relationship status and cell phone number) compared to those teens with a below-average SNS network size. In line with this result, another study observed that the level of information disclosure on a user's profile is positively related to the number of friends that the individual has on SNSs (Lampe, Ellison, and Steinfield 2007; Young and Quan-Haase 2009). Moreover, it is plausible that when adolescents provide a vast amount of information on their profiles, this will elicit more feedback from other users, thereby increasing the exposure of one's profile content to friends of friends. Therefore, we expect that:

H4b: There is a positive association between adolescents' level of disclosing information on SNSs and the number of friends they have on their profile.

2.3. Profile page experience

Some SNS users have been active on social media since the early days. The beginning era of SNSs is situated by Boyd and Ellison (2007) in the years 2002 and 2003 when, respectively, Friendster and MySpace were introduced. Others joined in later and have in this respect less experience with profile pages. Among young users of SNSs a *cohort effect* plays, in the sense that the cohort of adolescents currently about 13 years in age was very young when SNSs became popular. Due to their age, most of them have not been able to use SNSs until recently, when they were allowed to do so both from (1) a legal/self-regulatory perspective (e.g. COPPA; self-installed age requirements by a specific SNS) and/or (2) a family perspective (i.e. that they received the permission of their parents).

The association between the years that people have been active on SNSs (experience measured in terms of years) and the extent to which SNS users apply privacy settings has been the focus of attention in some studies. For instance, a study incorporating a four-wave longitudinal panel design conducted by Lewis (2011) uncovered a pronounced trend of more students adopting private profiles over time, indicating that accumulated experience in SNS use leads to a stricter application of privacy settings. Whereas in 2006 only 6.1% of undergraduate students had their profiles set to private, this share had risen to 40.3% in 2009.

However, other studies focusing on the influence of Internet experience in general on users' privacy attitudes and behaviours suggest an opposite effect, in that they found that an increase in computer knowledge and Internet experience leads to a decrease in respondents' level of privacy concern and a reduced motivation to protect their privacy (Bellman et al. 2004; Cho, Milagros, and Sun Sun 2009). The most recent Pew study showed a slight decrease in the share of adolescents having a private profile between 2011 (62%) and 2013 (60%) (Madden et al. 2013).

These opposing results may be explained by two different processes at work. On the one hand, greater experience with the Internet in general and social media in specific may lead to higher skills in protecting personal information. It may well be that with an increase in years of experience, users by practice get more skilled in protecting their profiles. The outcome of such a process would be that experienced users are more likely to use privacy settings than non-experienced users. On the other hand, some studies suggest that with more experience, users also tend to overestimate their feelings of online safety (Staksrud, Ólafsson, and Livingstone 2013). Such feelings may decrease a user's

willingness to further protect against online perils in general and privacy-related risks in specific. In this study, we follow the latter explanation. Therefore, we expect that:

H5a: The longer adolescents have been active on SNSs, the less they will protect the personal information on their profile.

Intergenerational research into people's use of SNSs has detected a higher likelihood (11 times higher, to be exact) that young users (15–30 years old) have more friends on SNSs than older users (those above 50 years) (Quinn, Liming, and Mulvenna 2011). Moreover, Joinson's study (2008) suggests that teenagers assign more importance to the number of friends displayed on their profiles than older users of SNSs.

The most recent study by the Pew Internet project provides more information on the *within-adolescence* differences in this area. Based on the data of this study, it seems that older teens (both males and females) tend to have more friends than younger teens (Madden et al. 2013). Many of these older teens have accumulated a larger degree of experience with SNSs compared to younger SNS-using teens. This may have provided them with more opportunities to extend their friend networks on SNSs. Hence, we expect that:

H5b: The longer adolescents have been active on SNSs, the more friends will be included on their SNS friends list.

3. Methods

3.1. Participants

In total, 1743 respondents (42.9% males; $M_{\text{age}} = 14.7$; $SD = 1.82$) from 16 different schools completed a questionnaire in November 2012. From a list provided by the Belgian Ministry of Education, we selected 28 schools situated in Antwerp to participate in our study. Of this initial convenience sample of 28 schools, 16 schools consented to participate in our study. The refusing schools did not participate because (a) they had already consented to participate in other academic studies or (b) there was not enough time available in the teaching schedules. From each participating school, three classes of pupils were selected to complete the questionnaire. Consent at respondent level was obtained before the pupils started completing the questionnaire. It was emphasised by the researcher administering the questionnaire that any pupil was free to choose whether or not to participate in the study. Except for pupils being absent at the moment of the data collection (mainly due to illness), all other pupils were prepared to participate in the study.

Respondents were between 12 and 18 years old. The distribution of respondent ages was more or less equally

spread, with students from each study year being proportionally represented in the sample (1st year students: $n = 282$; 2nd year students: $n = 299$; 3rd year students: $n = 314$; 4th year students: $n = 355$; 5th year students: $n = 227$; 6th year students: $n = 253$; 7th year students (optional year): $n = 11$). Respondents were recruited from the three different educational levels in the Belgian schooling system. About 9 in 10 (90.6%) adolescents involved in our sample had an active account on at least one SNS. Among these adolescents, Facebook was the predominant and most frequently used provider, with an overwhelming majority (91.9%) of respondents designating this SNS as their most used profile page. As the main component of the questionnaire dealt with questions regarding adolescents' SNS activities, only respondents reporting they had a profile page (Facebook, Hyves, Netlog or MySpace) were included in further analyses ($n = 1564$).

3.2. Measures

3.2.1. Level of disclosure on SNSs

This concept was measured by means of five items, all tapping into the question of how frequently people disclose a list of specific pieces of personal information on their profiles. Respondents could indicate their answer on a 5-point scale (*never* (= 1), *monthly* (= 2), *weekly* (= 3), *daily* (= 4), *many times per day* (= 5)). In this way, we used frequency of SNS disclosure as a proxy for the way adolescents protect their profile by modulating their level of SNS disclosure. The scale was reliable (Cronbach's alpha: .76).

3.2.2. Use of privacy settings

Respondents were asked to indicate what privacy settings they had applied for each of the listed categories of personal data. Respondents could indicate their answer on a 6-point scale with the following answer categories: the information is visible to (...) *everyone* (= 1), *friends of friends* (= 2), *friends* (= 3), *customised settings* (= 4), *only me* (= 5) or *I do not disclose this information* (= 6).

3.2.3. Audience management

We operationalised this variable by asking respondents how large the audience (in terms of accepted friends) was on the profile page they used most: (*less than 50* (= 1), *between 51 and 100* (= 2), *between 101 and 200* (= 3), *between 201 and 300* (= 4), *between 301 and 400* (= 5), *between 401 and 500* (= 6) or *more than 500* (= 7)).

3.2.4. Need for popularity

The items for the *need-for-popularity* scale were based on a scale validated in prior research (Santor, Messervey,

and Kusumakar 2000). Eight items were measured on a 6-point Likert scale ranging between *totally disagree* (= 1) and *totally agree* (= 6) (e.g. 'I have done things to make me more popular, even when it meant doing something I would not usually do'; 'I've neglected some friends because of what other people might think'). Analyses performed in SPSS demonstrate that the scale was highly reliable (Cronbach's alpha: .85).

3.2.5. Motivation to meet new people

This concept was measured by using three items on a 5-point Likert scale anchored by *totally disagree* (= 1) and *totally agree* (= 5) (e.g. I use my profile page to meet new people and to make friends). The scale was reliable (Cronbach's alpha: .70).

3.2.6. Profile page experience

This variable was operationalised by asking adolescent respondents how long they had been active on SNSs at the timing of the questionnaire. Respondents could answer by indicating one of the available answering categories (*less than six months* (= 1), *between six months and one year* (= 2), *between one and two years* (= 3), *between two and three years* (= 4), *between three and four years* (= 5), *between four and five years* (= 6) or *more than five years* (= 7)).

3.3. Data analysis

Structural equation modelling (SEM) was applied to the data by using Mplus 6 (Muthén and Muthén 2010). We analysed the data using a two-step approach. We first assessed a measurement model in order to establish whether the observed variables reliably reflect the hypothesised latent constructs in the model. Thereafter, we added the structural paths to the model in order to assess the adequacy with which the research model predicts adolescents' privacy management on SNSs. In our model, respondents' use of privacy settings and number of friends were entered as endogenous variables. MLR was used as an estimator in SEM analyses, which is an Mplus option for maximum likelihood estimation with robust standard errors (Muthén and Muthén 2010).

4. Results

4.1. Descriptive results

With respect to adolescents' use of privacy settings, we can derive from Table 1 that a majority of teens have restricted the largest part of their profile to friends only and that a minority of respondents opens up their profile to everyone: About one in ten adolescents (10%) allows

Table 1. Cross-tabulation of use of privacy settings by adolescent respondents.

| | | Status update (%) | Identity data (%) | E-mail (%) | Mobile phone number (%) | Pictures (%) | Place to live (%) | Hobbies (%) |
|---------------------------|-------------------------------|-------------------|-------------------|------------|-------------------------|--------------|-------------------|-------------|
| Level of privacy settings | I do not give the information | 11.5 | 5.1 | 20.6 | 53.7 | 3.8 | 35.7 | 10.6 |
| | Only me | 2.4 | 6.5 | 22.8 | 22.3 | 2.1 | 13.1 | 3.5 |
| | Friends | 55.2 | 52.5 | 40.8 | 17.1 | 61.1 | 35.1 | 54.0 |
| | Customised | 5.0 | 4.1 | 2.2 | 1.9 | 5.0 | 2.2 | 2.4 |
| | Friends of Friends | 12.9 | 12.5 | 5.2 | 1.7 | 16.4 | 5.7 | 13.0 |
| | Everyone | 8.5 | 16.4 | 4.1 | 1.2 | 9.7 | 4.5 | 12.8 |
| | I do not know | 4.6 | 2.9 | 4.2 | 2.0 | 2.0 | 3.7 | 3.7 |

everyone to access the pictures on their profile page. Very few adolescents in our sample reported using more fine-grained privacy settings, allowing a division of one's friends list into groups with varying degrees of privacy and access; only 5% reported doing this to limit access to their pictures.

Our study shows that about one in eight adolescent SNS users (12%) have less than 100 friends. One in three adolescents (34%) indicated that the size of their SNS network balances between 100 and 300 friends, whereas one in four adolescents (27%) have a larger network on SNSs with more than 300 and less than 500 friends. For one in five (21%) students, the number of SNS friends exceeds the threshold of 500. Do adolescents only include people they know from offline environments on their friends list? Our study shows that one in three teenagers (35%) state that they have met all their SNS friends in the offline world, while about two in three adolescents (65%) report having SNS friends whom they have never met offline.

4.2. Measurement model

Table 2 displays the correlations between the latent constructs in the model. The SEM analyses revealed a good fit of the measurement model with the data: $\chi^2(183): 682.275$; comparative fit index: .933; Tucker-Lewis index: .924; root mean square error of approximation: .042 (confidence interval 90%: .038–.045); standardized root mean square residual: .038. All factor loadings were significant and above .391 (see Table 3).

4.3. Structural model

The structural model fit the data well (see bottom section of Figure 2). Although Chi-square was significant, other

Table 2. Zero-order correlations between latent constructs.

| Measures | 1 | 2 | 3 | 4 |
|--|-------|-------|-------|-------|
| 1. Motivation to meet new people on SNSs | 1.000 | | | |
| 2. SNS disclosure | .322 | 1.000 | | |
| 3. Privacy settings use | -.314 | -.391 | 1.000 | |
| 4. NFP | .406 | .151 | -.165 | 1.000 |

Note: $N = 1564$.

fit indices less susceptible to large sample size point to a good fit of the model with the data.

Testing the hypothesised paths in the model demonstrates that adolescents' need to be popular among peers (NFP) significantly predicted their motivation to meet new people (H1a). No significant path, however, could be observed between NFP and the extent to which adolescents disclose personal information about themselves. Therefore, H1b has to be rejected. The more adolescents were motivated to use SNSs for the purpose of getting acquainted with new people, the more frequently they were inclined to disclose their personal data on SNSs. This confirms hypothesis 2.

The expected negative association between adolescents' motivation to meet new people on SNSs and the level to which they protect the information contained in their profile by means of privacy settings was also confirmed (H3a). Adolescents who report using SNSs for meeting new people share a decreased likelihood of

Table 3. Results for measurement model: unstandardised and standardised parameter estimates.

| Observed variable | Latent construct | β | B | SE | Two-tailed p -value |
|----------------------------|-------------------------------|---------|-------|------|-----------------------|
| Mot_Item1 | Motivation to meet new people | .815 | 1.000 | .000 | |
| Mot_Item2 | | .851 | .944 | .039 | .000 |
| Mot_Item3 | | .436 | .618 | .045 | .000 |
| Disclosure: status updates | SNS disclosure | .749 | 1.000 | .000 | |
| Disclosure: pictures | | .678 | .618 | .037 | .000 |
| Disclosure: music | | .580 | .691 | .040 | .000 |
| Disclosure: wall messages | | .708 | .886 | .043 | .000 |
| Data: status updates | Use of privacy settings | .558 | 1.000 | .000 | |
| Data: identity data | | .551 | .940 | .070 | .000 |
| Data: e-mail address | | .393 | .791 | .084 | .000 |
| Data: pictures | | .671 | .914 | .063 | .000 |
| Data: place where I live | | .408 | .903 | .089 | .000 |
| Data: hobbies | | .608 | 1.130 | .088 | .000 |
| Needpop_item1 | NFP | .577 | 1.000 | .000 | |
| Needpop_item2 | | .565 | .991 | .052 | .000 |
| Needpop_item3 | | .619 | 1.264 | .072 | .000 |
| Needpop_item4 | | .744 | 1.239 | .066 | .000 |
| Needpop_item5 | | .799 | 1.407 | .070 | .000 |
| Needpop_item6 | | .418 | .928 | .075 | .000 |
| Needpop_item7 | | .684 | 1.108 | .067 | .000 |
| Needpop_item8 | | .788 | 1.186 | .063 | .000 |

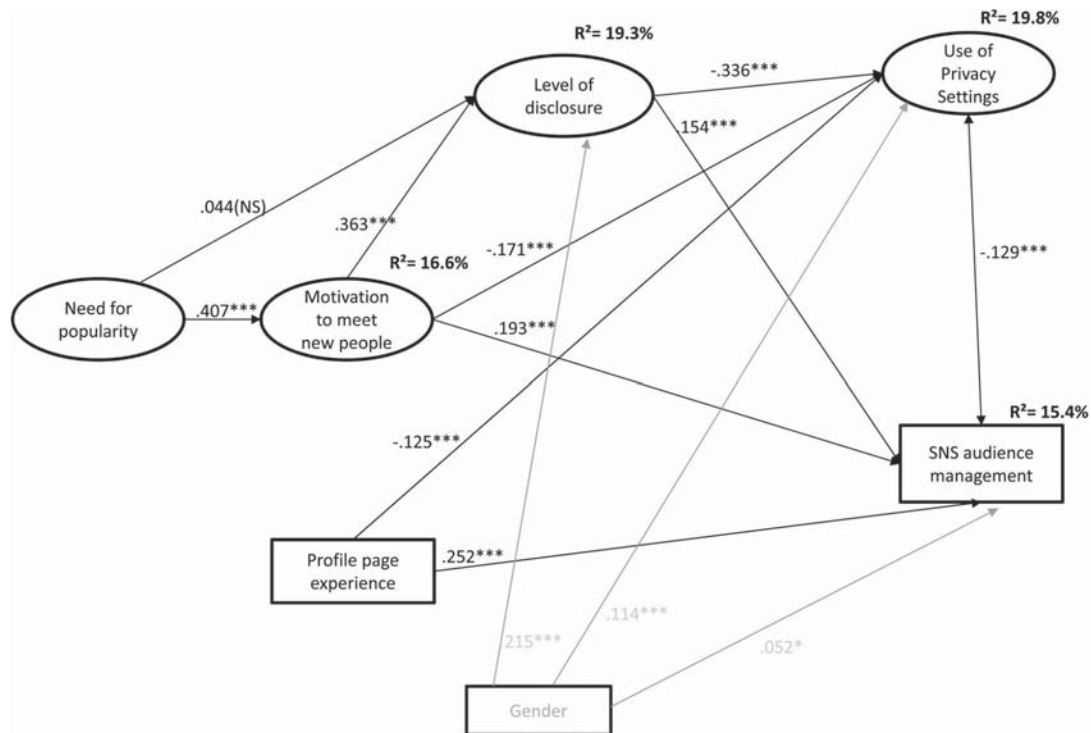


Figure 2. Structural model.

applying privacy settings, opposed to adolescents not especially interested in extending their social network by means of SNSs. Also, in line with our expectations, the analyses yielded a significant positive association between adolescents' use of SNSs for seeking new contacts and the number of contacts included in their SNS friends list (H3b).

A crucial finding of our study is that the predicted association between level of disclosure and the two other strategies of privacy protection on SNSs was confirmed. The more frequently adolescents disclose personal data on their profile page, the less inclined they are to protect these data by means of privacy settings (H4a) and the more friends they report having on SNSs (H4b). These results confirm that the multi-mechanic nature of offline privacy regulation as conceived by Altman also applies to privacy regulation in the online context.

As a final result, our study reveals a negative association between profile page experience and the extent to which users protect their profiles by means of privacy settings (H5a). The longer users have been active as SNS users, the less inclined they are to protect their profiles by using privacy settings. Moreover, a positive association was observed between profile page experience and the number of friends that adolescents have on SNSs (H5b): the longer they have been active on SNSs, the more likely they have a large amount of contacts included as friends in their profile. Finally, our

analyses revealed a negative correlation between adolescents' use of privacy settings and the number of friends included in their profile.

Analyses for the structural model were controlled for the demographic variables age and gender, but only for gender we observed a significant association with the endogenous variables in the model (see the grey arrows in the model). Age was not significantly associated with any of the outcome variables, which was probably due to the fact that all respondents belong to a relatively small age span of six years (between 12 and 18 years old). We decided to drop age out of the model, given that its inclusion caused a significant deterioration of the model fit as reflected by the fit indices displayed in Figure 2.

In short, given the outcomes of our analyses, the findings provide evidence that adolescents' privacy-protective strategies on SNSs indeed work as a system. Adolescents' level of disclosure on SNSs partially determines the settings they will apply to their profile content and the size of the audience that will be able to consult this information.

5. Conclusion and discussion

The aim of the present study was to examine how three privacy-protective online strategies – disclosure management, control by privacy settings and SNS audience management – relate to one another. Our study supports

Altman's (1977) idea that privacy-protective regulation strategies operate as an interdependent system. The central idea of his theory, conceived of long before the dawn of online technology, is therefore also applicable to an SNS environment. Adolescents, in their attempt to protect the personal information contained in their SNS profiles, are likely to adopt a mix of privacy-regulating strategies. More specifically, this study demonstrates that adolescents' privacy management on SNSs is the result of the following decision-making process: Adolescents decide which type of personal details they are willing to disclose. The outcome of this decision is associated with the technological and social choices they make, as they respectively choose what privacy settings they prefer for their content and the extent of the audience that has immediate access to their personal information (mirrored in the number of accepted friends). Those adolescents with low frequency of information disclosure on SNSs were found to set the content of their SNS profiles to more restrictive access compared to those adolescents frequently disclosing their personal data. This finding challenges the findings by Christofides, Muise, and Desmarais (2009), who found no significant relation between level of disclosure and control on Facebook and, therefore, considered both strategies as different processes.

In addition, those adolescents frequently disclosing data on SNSs are more likely to have a large number of friends on SNSs. A possible explanation for this result may be that profiles containing a lot of information about a person are more attractive and *interest-eliciting* from the perspective of outsiders who are not yet friended with the adolescent profile owner. It is plausible that profiles that are never or rarely updated with *fresh* status updates will attract relatively less attention from potential new friends. In this regard, our study supports findings from earlier studies that observed a similar positive relationship between level of disclosure and the number of friends one has on SNSs (e.g. Madden et al. 2013).

In the introduction, we noted that early research on the relation to be expected between profile page experience and the use of privacy settings yielded mixed findings. In line with, for instance, Mesch and Beker (2010), our study also provides further indications that experience with online tools and platforms (including SNSs) rather decreases users' inclination to protect their online safety. More experienced adolescent Internet users reported lower levels of privacy protection by means of privacy settings compared to relatively less experienced users. This finding can possibly be explained by the fact that experienced adolescent Internet users tend to have a lot of confidence in their ICT-related capacities, which subsequently attenuates their motivation to apply privacy-protective measures. The positive relation

between the number of years active on SNSs and the number of friends included in one's profile is not entirely surprising as more years of SNS use elicits more occasions to perform friending behaviours.

Some limitations have to be acknowledged. The foremost weakness of this study is the cross-sectional nature of the dataset, impeding us from making firm causal claims. Therefore, we cannot fully exclude the possibility that some of the observed relationships go in the opposite direction of what the hypotheses predict: It is possible that adolescents' use of privacy settings and their choices with respect to SNS audience management partially affect their SNS disclosure behaviours. A longitudinal study or experimental research design could be deployed to provide further support for the directionality of the observed relationships in our study. Such research designs can verify the plausibility of a scenario in which the use of privacy settings triggers disclosure on SNSs. The rationale behind such an association could be that adolescents are falsely convinced that privacy settings work as a *silver bullet* for protecting their privacy on SNSs and thereby feel more disinhibited to freely disclose information online. Another limitation is that the list of privacy-enhancing strategies on SNSs is not exhaustive. SNS users in general and adolescents in particular can conceive of other ways to protect the information contained in their profiles. Examples of such alternative privacy-protective strategies are online steganography (the use of enigmatic language to 'hide information in plain sight') or deliberately falsifying personal information on one's profile. One additional way to protect information on SNSs is the careful selection of public vs. private communication channels on SNSs. The visibility of an SNS communication channel varies between two extremes: *public SNS channels* (e.g. status updates on one's profile *wall*) vs. *private SNS channels* (e.g. messages in the private chat function). Future studies could investigate these specific SNS channels as specific strategies to communicate more privately.

Notwithstanding some shortcomings, this study contributed to the current literature in several ways. The strength of this study resides in the integration of the hypothesised relationships within one comprehensive model. Moreover, opposed to earlier studies examining adolescents' use of privacy settings, our questionnaire did include questions regarding more fine-grained customised privacy settings that are available on SNSs (e.g. on Facebook since 2009). These customised options allow users to further differentiate among SNS friends who get full access to the information posted on one's profile and who only get partial access. According to recent American research (Madden et al. 2013), only a few adolescents (18%) choose to customise and differentiate the

privacy settings between their SNS friends in this way. This low rate of adolescents with custom privacy settings is confirmed in our study with only a marginal share of respondents using these advanced types of privacy settings. Two explanations can be provided for this result: First, customising privacy settings to create different zones of privacy on SNSs requires time and cognitive efforts from adolescents, and possibly only a minority of adolescents is willing to spend their leisure time to explore how to adequately protect their profile content in an advanced way. Second, driven by their business model, SNS providers want to stimulate adolescents to disclose as much information as possible and to keep this information as public as possible (Pekárek and Leenes 2009). A fruitful strategy to prevent SNS users from applying advanced privacy settings is keeping the process to do so as difficult as legally possible (Papacharissi and Gibson 2011). Hence, it is not surprising that applying customised privacy settings is a difficult task, even for adults, as has been proven in several studies (Stutzman and Kramer-Duffield 2010). In order to enhance the application of customised privacy settings among members of the adolescent age group, several fruitful venues could be pursued: First, teachers could be instructed by a privacy expert and hereby trained to demonstrate to their pupils how to adequately protect their personal information on SNSs by enabling a differentiation of access between SNS friends. Second, privacy experts themselves could be invited to schools to demonstrate to pupils how to do this. The latter strategy has the advantage that no information is being lost (as could be the case when teachers serve as indirect transmitters of the instructions) and that pupils are perhaps more likely to follow the instructions of an expert. Both ways of informing have the potential to lower the threshold – in terms of cognitive efforts required – for engaging in customising privacy settings. Given that these instructions are provided during school time, it is less likely that pupils will experience them as a loss of their valuable leisure time.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Research Foundation Flanders (FWO) [grant number FWO G047415N].

References

- Altman, Irwin. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues* 33 (3): 66–84.
- Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20 (5): 313–324.
- Boyd, danah. 2008. *Taken Out of Context: American Teen Sociality in Networked Publics* (Doctor of Philosophy). Berkeley: University of California.
- Boyd, danah, and Nicole B. Ellison. 2007. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13 (1): 210–230. doi:10.1111/j.1083-6101.2007.00393.x
- Buhrmester, Duane, and Karen Prager. 1995. "Patterns and Functions of Self-Disclosure During Childhood and Adolescence." In *Disclosure Processes in Children and Adolescents*, edited by Ken J. Rotenberg, 10–57. Cambridge: Cambridge University Press.
- Chang, Chen-Wei, and Jun Heo. 2014. "Visiting Theories that Predict College Students' Self-disclosure on Facebook." *Computers in Human Behavior* 30: 79–86.
- Cho, Hichang, Rivera-Sánchez Milagros, and Lim Sun Sun. 2009. "A Multinational Study on Online Privacy: Global Concerns and Local Responses." *New Media and Society* 11 (3): 395–416.
- Christofides, Emily, Amy Muise, and Serge Desmarais. 2009. "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *CyberPsychology and Behavior* 12 (3): 341–345.
- Christofides, Emily, Amy Muise, and Serge Desmarais. 2010. *Privacy and Disclosure on Facebook: Youth and Adults' Information Disclosure and Perceptions of Privacy Risks*. Guelph: University of Guelph.
- Christofides, Emily, Amy Muise, and Serge Desmarais. 2012. "Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior." *Journal of Adolescent Research* 27 (6): 714–731.
- Debatin, Bernhard. 2011. "Ethics, Privacy, and Self-Restraint in Social Networking." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 47–61. Heidelberg: Springer.
- Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15 (1): 83–108. doi:10.1111/j.1083-6101.2009.01494.x.
- Ellison, Nicole B., Charles Steinfield, and Cliff Lampe. 2007. "The Benefits of Facebook 'Friends': Social Capital and College Students' Use of Online Social Network Sites." *Journal of Computer-Mediated Communication* 12 (12): 1143–1168.
- Ellison, Nicole B., Charles Steinfield, and Cliff Lampe. 2011. "Connection Strategies: Social Capital Implications of Facebook-Enabled Communication Practices." *New Media and Society* 13 (6): 873–892. doi:10.1177/1461444810385389.
- Ellison, Nicole B., Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 19–32. Berlin: Springer-Verlag.

- Hasebrink, Uwe, Sonia Livingstone, and Leslie Haddon. 2008. *Comparing Children's Online Opportunities and Risks Across Europe: Cross-National Comparisons for EU Kids Online*. London: EU Kids Online.
- Hoek, Janneke, Paula O'Kane, and Martin McCracken. 2016. "Publishing Personal Information Online: How Employers' Access, Observe and Utilise Social Networking Sites Within Selection Procedures." *Personnel Review* 45 (1): 67–83. doi:10.1108/PR-05-2014-0099.
- Jang Hyun, Kim, Kim Min-Sun, and Nam Yoonjae. 2010. "An Analysis of Self-Construals, Motivations, Facebook Use, and User Satisfaction." *International Journal of Human-Computer Interaction* 26 (11/12): 1077–1099. doi:10.1080/10447318.2010.516726.
- Joinson, Adam N. 2008. "Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook." Paper presented at the CHI, Florence, Italy.
- Kim, Yoojung, Dongyoung Sohn, and Sejung M. Choi. 2011. "Cultural Difference in Motivations for Using Social Network Sites: A Comparative Study of American and Korean College Students." *Computers in Human Behavior* 27 (1): 365–372. doi:10.1016/j.chb.2010.08.015.
- Krasnova, Hanna, and Natasha F. Veltri. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA." Paper presented at the 43rd Hawaii International Conference on System Sciences, Hawaii.
- Lampe, Cliff, Nicole Ellison, and Charles Steinfield. 2007. "A Familiar Face(book): Profile Elements as Signals in an Online Social Network." Paper presented at the CHI 2007, San Jose, CA.
- Lampinen, Airi, Sakari Tamminen, and Antti Oulasvirta. 2009. "All My People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site." Paper presented at the proceedings of the ACM 2009 international conference in Florida, USA.
- Lenhart, Amanda, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, and Lee Rainee. 2011. *Teens, Kindness and Cruelty on Social Network Sites*. Washington, DC: Pew Internet.
- Lewis, Kevin. 2011. "The Co-evolution of Social Network Ties and Online Privacy Behavior." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 91–111. Heidelberg: Springer.
- Lin, Nan, Karen S. Cook, and Ronald S. Burt. 2008. *Social Capital: Theory and Research*. New Brunswick, NJ: Transaction.
- Livingstone, Sonia, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. *Risks and Safety on the Internet: The Perspective of European Children. Full Findings*. London: LSE.
- Madden, Mary, Sandra Cortesi, Urs Gasser, Amanda Lenhart, and Maeve Duggan. 2012. *Parents, Teens, and Online Privacy*. Washington, DC: Pew Internet and American Life Project.
- Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. 2013. *Teens, Social Media, and Privacy*. Washington, DC: Pew Internet and American Life Project.
- Marwick, Alice E., and danah Boyd. 2011. "I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience." *New Media and Society* 13 (1): 114–133. doi:10.1177/1461444810365313.
- Mesch, Gustavo S., and Guy Beker. 2010. "Are Norms of Disclosure of Online and Offline Personal Information Associated with the Disclosure of Personal Information Online?" *Human Communication Research* 36 (4): 570–592. doi:10.1111/j.1468-2958.2010.01389.x.
- Muthén, Linda, and Bengt Muthén. 2010. *Mplus Users' Guide: Sixth Edition*. Los Angeles: Muthén & Muthén.
- Ong, Eileen Y. L., Rebecca P. Ang, Jim C. M. Ho, Joylynn C. Y. Lim, Dion H. Goh, Chei Sian Lee, and Alton Y. K. Chua. 2011. "Narcissism, Extraversion and Adolescents' Self-presentation on Facebook." *Personality and Individual Differences* 50: 180–185. doi:10.1016/j.paid.2010.09.022.
- Oolo, Egle, and Andraa Siibak. 2013. "Performing for One's Imagined Audience: Social Steganography and Other Privacy Strategies of Estonian Teens on Networked Publics." *CyberPsychology: Journal of Psychosocial Research in Cyberspace* 7 (1). <http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501>
- Papacharissi, Zizi, and Paige L. Gibson. 2011. "Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 75–91. Heidelberg: Springer.
- Pekárek, Martin, and Ronald Leenes. 2009. "Privacy and Social Network Sites: Follow the Money." Paper presented at the W3C Workshop, Barcelona, Spain.
- Pelling, Emma L., and Katherine M. White. 2009. "The Theory of Planned Behavior Applied to Young People's Use of Social Networking Web Sites." *CyberPsychology and Behavior* 12 (6): 755–759.
- Peter, Jochen, and Patti M. Valkenburg. 2011. "Adolescents' Online Privacy: Toward a Developmental Perspective." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by S. Trepte and L. Reinecke, 221–234. Heidelberg: Springer.
- Putnam, Robert D. 2000. *Bowling Alone*. New York: Simon & Schuster.
- Quinn, Darren, Chen Liming, and Maurice Mulvenna. 2011. "Does Age Make a Difference in the Behaviour of Online Social Network Users?" Paper presented at the Internet of Things (iThings/CPSCOM), 2011 International Conference, Dalian, China.
- Rotenberg, Ken J. 2006. *Disclosure Processes in Children and Adolescents*. Cambridge: Cambridge University Press.
- Russon, Mary-Ann. 2015. "US Court Rules Private Facebook Profile Can Be Used as Evidence in Custody Battle." *International Business Times*. Accessed August 26, 2015. <http://www.ibtimes.co.uk/us-court-rules-private-facebook-profile-can-be-used-evidence-custody-battle-1517172>.
- Santor, Darcy A., Deanne Messervey, and Vivek Kusumakar. 2000. "Measuring Peer Pressure, Popularity, and Conformity in Adolescent Boys and Girls: Predicting School Performance, Sexual Attitudes, and Substance Abuse." *Journal of Youth and Adolescence* 29 (2): 163–182. doi:10.1023/a:1005152515264.
- Siibak, Andraa. 2009. "Constructing the Self Through the Photo Selection – Visual Impression Management on Social Networking Websites." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3 (1), article 1.

- Slavtcheva-Petkova, Vera, Monica Bulger, and Victoria Jane Nash. 2013. "Evidence of the Extent of Harms Experienced by Children as a Result of Online Risks: A Critical Synthesis of Research". Paper presented at the ICA, London.
- Spiekermann, Sarah, Hannah Krasnova, Ksenia Koroleva, and Thomas Hildebrand. 2010. "Online Social Networks: Why We Disclose." *Journal of Information Technology* 25 (2): 109–125.
- Staksrud, Elisabeth, Kjartan Ólafsson, and Sonia Livingstone. 2013. "Does the Use of Social Networking Sites Increase Children's Risk of Harm?" *Computers in Human Behavior* 29: 40–50. doi:10.1016/j.chb.2012.05.026.
- Steinberg, Laurence D. 2011. *Adolescence. 9th International Edition*. New York: McGraw-Hill Humanities.
- Stutzman, Fred, and Jacob Kramer-Duffield. 2010. "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook." Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, New York.
- Utz, Sonja, Martin Tanis, and Ivar Vermeulen. 2012. "It Is All about Being Popular: The Effects of Need for Popularity on Social Network Site Use." *Cyberpsychology, Behavior and Social Networking* 15 (1): 37–42. doi:10.1089/cyber.2010.0651.
- Valkenburg, Patti M., Jochen Peter, and Alexander P. Schouten. 2006. "Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem." *CyberPsychology and Behavior* 9 (5): 584–590.
- Walrave, Michel, Ini Vanwesenbeeck, and Wannes Heirman. 2012. "Connecting and Protecting? Comparing Predictors of Self-disclosure and Privacy Settings Use between Adolescents and Adults." *CyberPsychology* 6 (1), article 3. doi:10.5817/CP2012-1-3.
- Weinstein, Carol, Thomas Simon, and G. David. 1987. *Spaces for Children: The Built Environment and Child Development*. New York: Plenum Press.
- Wilson, Robert E., Samuel D. Gosling, and Lindsay T. Graham. 2012. "A Review of Facebook Research in the Social Sciences." *Perspectives on Psychological Science* 7 (3): 203–220. doi:10.1177/1745691612442904.
- WIP. 2013. *World Internet Project 2013: International Report*. 5th ed. Los Angeles: World Internet Project.
- Young, Alyson L., and Anabel Quan-Haase. 2009. "Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook." Paper presented at the fourth international conference on communities and technologies.
- Young, Alyson L., and Anabel Quan-Haase. 2013. "Privacy Protection Strategies on Facebook." *Information, Communication and Society* 16 (4): 479–500. doi:0.1080/1369118X.2013.777757.