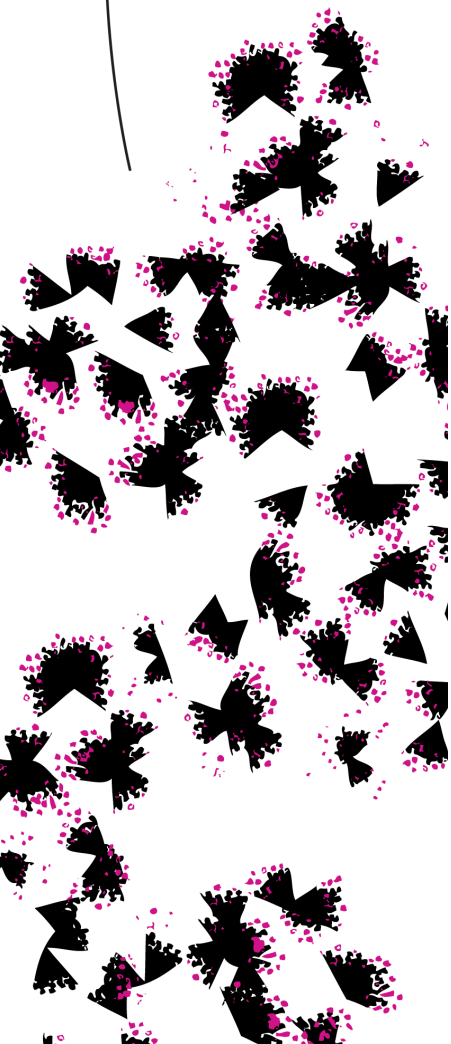
Personal Information Disclosure on Online Social Networks

An empirical study on the predictors of adolescences' disclosure of personal information on Facebook



Master thesis report Communication Studies

Department of Communication Science
University of Twente, Enschede

Ruud H.G. Koehorst
August 23rd, 2013

Supervisors: Dr. A. Beldad and Dr. J.M. Gutteling

ABSTRACT

This report discusses the results of an empirical study on the predictors of an individuals' intention to disclose personal information on online social networks (*OSNs*). After filtering out the respondents that were prone to give social desirable answers, linear regression analysis on the remaining data showed that the respondents' (n = 491) habits were the strongest significant predictor for one's intention to disclose personal information on OSNs. Subsequently, there is a significant influence of the benefits of sharing personal information and the perceived control over this personal information on the intention to disclose personal information on OSNs. In addition, it was found that there was a causal relationship between both the trusting beliefs concerning disclosed personal information and the perceived control over this information, and the respondents' privacy valuation.

Keywords: personal information disclosure; online social networks; privacy valuation; habits; social desirable responding

TABLE OF CONTENT

" Nobody is literally forced to join an online social network, and most networks we know about encourage, but do not force users to reveal personal information. And yet, one cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed this information sharing is."

—Acquisti & Gross (2006, p. 37)

1 Introduction

An increasing number of people are pushed to second lives in the digital world and people, in one way or another, have to battle with information privacy concerns, since participation in online exchanges and communication entail the disclosure of private information. Despite existing threats like privacy issues, potential for misuse of data, unwanted access to information, risk for child safety and online bullying, and negative psychological effects of social networking, people continue to reveal massive amounts of personal information on *online social networks* (OSNs).

One might wonder: do users of OSNs actually value their privacy? What are the antecedents of this privacy valuation and how does this affect their perception of privacy risks as a result of the personal information they disclose? And do other factors exist that might affect the intention to disclose personal information on OSNs?

In his book 'The Network Society', Van Dijk (2012) mentions eight social and personal effects of OSNs, including the blurring of traditional dividing lines in life and communication, the dilemma of privacy and the disclosure of identity, and social pressure and addiction (p. 185). These issues are of public interest, and in the last 25 years there has been an ongoing debate whether or not the internet decreases human sociability. In The Netherlands, 96% of the population has internet access, and 77% of this group uses OSNs. Users of OSNs post messages (55%), react to 'status updates' (63%), keep their profile up-to-date (46%), and share pictures (29%) at least once a week (Van Deursen & Van Dijk, 2012).

Even though more recent observations of social media use are also in favor of the positive effects that the internet has on people (Van Dijk, 2012, p. 186; Van Deursen & Van Dijk, 2012), the issues concerning privacy and information disclosure on OSNs are still of increasingly interest of researchers and users (e.g. O'Brien & Torres, 2012; Davis & James, 2012).

The continuous and fast developments of OSNs (and other options to share personal information through digital media) and the technologies that enables individuals to use these services requires ongoing attention from researchers. It is the main objective of this study to gain more insight in what drives users of online social networks to disclose personal information.

Structure of the Research Report

The following chapter is the *Theoretical Framework*. This chapter covers the articles that were the foundation for this report, and it will discuss other literature that covers the different concepts that are important to personal information disclosure, and formulate research questions and hypotheses along the path. Chapter 3 will describe the *Research Method*, and discusses the choice of OSN and respondents and explains the item sets that were used to measure the seven variables. Additionally, it explains the importance of social desirable responses. The next chapter displays the *Results*. It starts with the results from the social desirability test, describes the demographics of the respondents and their tendency to falsify information. The remainder of the chapter is dedicated to the different statistical analyses that has been done. Chapter 5, the *Discussion*, discusses the results and how this relates to the findings from the literature research. The chapter ends with the conclusion that can be drawn, based on the research-data. The next chapter, *Recommendations and Implications*, is self-explanatory and provides practical and theoretical implications and recommendations for further research. In the final chapter, *Acknowledgments*, the individuals and organizations that contributed to this research are thanked.

2 Theoretical Framework

Research about disclosure of personal information often focusses on the commercial, healthcare, or governmental settings (e.g. Phelps, Nowak & Ferrell, 2000; Culnan & Armstrong, 1999; Gostin, Turek-Brezina, Powers, Kozloff, Faden & Steinauer, 1993). Despite many similarities that OSNs have with these environments, Xu, Dinev, Smith and Hart (2008) state OSNs have significantly distinctive characteristics which may prove relevant to personal information disclosure, like personal information which is often publicly accessible and the lack of autonomy as a result. Online social networks are a relatively new phenomenon on the internet and are currently among the most popular websites on the internet.

Boyd (2009) argues that OSNs are a type of networked public, but with four properties that are not common in face-to-face public life and communication: persistence, searchability, replicability, and invisible audiences (p. 120). This causes social dynamics to be fundamentally different in comparison to other areas and complicate the way people interact.

While these social networking sites all have the basic purpose of online interaction and communication in common, specific goals and patterns of usage vary significantly across different services. The most common models are based on the presentation of the participant's profile, the visualization of her network of relations to others, contain category places, and allow the users to communicate with each other across political, economic, and geographic borders (Gross & Acquisti, 2005).

Existing academic research on the effects of information disclosure on OSNs has focused on social capital (e.g. Ellison, Steinfield, & Lampe, 2007), identity presentation (e.g. Stutzman, 2006), and (benefits for) electronic commerce (e.g. Hui, Tan, & Goh, 2006). However, most academic research addresses the issues that come with the global popularity of OSNs, like privacy issues (e.g. Debatin, Lovejoy, Horn & Hughes, 2009; Gross & Acquisti, 2005), potential for misuse like *data mining* and unwanted access to information (e.g. Clarke, 1999; Strater & Richter, 2007), risk for child safety and online bullying (e.g. Staksrud & Livingstone, 2009; Lwin, Stanaland & Miyazaki, 2008; Youn, 2005), and negative psychological effects of social networking services (Youn, 2005, Krasnova, Kolesnikova & Günther, 2009).

This report will use two articles as the foundation of this research. Beldad, De Jong, and Steehouder (2011) provide a solid basis with their theoretical framework for information-related behaviors on the internet. In their literature research, Beldad *et al.* mention the influence of benefits, trust, risk perception, and habits on personal information disclosure or protection behavior. In addition, the authors note the role of privacy concerns on risk perception, and the influence privacy assurances and security features have on trust.

Because this article does not specifically focus on OSNs, the findings and the proposed model are combined with the findings of Krasnova, Spiekermann, Koroleva, and Hildebrand (2010). This study, on why individuals disclose, empirically tests the role of four different types of benefits and perceived privacy risk on self-disclosure. In addition, they test how perceived control influences perceived privacy risks and trust in the OSN provider and users.

The first step in understanding the antecedents of personal information disclosure behavior on OSNs is to formulate the following research question:

RQ: How do the habits of sharing personal information, the benefits of sharing this information, the perceived privacy risks of this information, the individuals' valuation of privacy, the trust in parties the information is shared with, and the perceived control over the personal information shared on an OSN affect an individuals' intention to disclose personal information on OSNs?

In addition, Beldad, De Jong, and Steehouder (2010) state that "when people trust, they are increasing their vulnerability to others whose behavior they cannot control." (p. 859). Increasing your own vulnerability increases the value one attaches to the trusting behavior. In other words, the more an individual is confident that his or her personal information will be handled competently, reliably, and safely (i.e., *trusting beliefs*), the more this individual values the

privacy which they think these trusting beliefs results in. As with the reasoning behind the influence of trust on privacy valuation, it is theorized that a perception of being in control increases the value an individual attaches to this sense of being in control of their personal information. If an individual has no means to control the selective disclosure, nor the right to select contacts without observation and intrusion, there is no reason to attach any value to the privacy of the disclosed information. In other words: the more an individual is confident that he or she is in control of their personal information, the more this person values the privacy which they perceive this control gives them.

Although there is no substantial theoretical evidence in recent literature to support the hypothesis that there is a causal relation between trust and perceived control and privacy valuation, the aforementioned reasoning provides sufficient support to explore the following research subquestion:

RSQ: How does an individuals' a) trusting beliefs concerning disclosed personal information on OSNs, and b) perceived control over this information, influence their privacy valuation?

We will start this chapter with the conceptualization of personal information disclosure and its determinants. This will result in a set of hypotheses and a conceptual model that corresponds with the theoretical framework.

2.1 Personal Information Disclosure

The term 'disclosure' can be seen as a fluid term that often changes among researchers (Waters & Ackerman, 2011). Joinson and Payne (2007) offer a reflective definition explaining the core of disclosure: "the telling of the previously unknown so that it becomes shared knowledge" (p. 235). This is in line with the definition of self-disclosure, or personal information disclosure, by Wheeless & Grotz (1976, p. 47) who defined it as "any message about the self that a person communicates to another" (as cited by Krasnova *et al.*, 2010).

This research paper will combine both definitions for 'disclosure', and make an adjustment to the term 'personal information'. Apart from textual (e.g. messages, likes, tags) and graphical (e.g. pictures, video) personally identifiable information, OSN users also reveal other information such as hobbies, taste in music, books and movies, relationship status, sexual preference, and family connections on their profiles (Gross & Acquisti, 2005). Thus, in this report, personal information disclosure is operationalized as "any form of information about the self that a person makes shared knowledge".

Waters and Ackerman (2011) note that most common definitions of self-disclosure assumes that a recipient of the information must be present. According to Van Dijk (2012, p. 40) "it is easy to speak on the internet, but difficult to be heard". The author theorizes that due to the large amount of senders in typical social media services, but limited time of the individuals that receive all the messages, most of the information shared has a very small audience, if any (p. 41). However, in the context of OSNs it is theorized that every message that is shared has a recipient; if none of the OSN-contacts (consciously) receives the information, the information will be received trough any form of 'dataveillance' (e.g. Clarke, 1999; Ashworth & Free, 2006), database-mining (e.g. Schoenbachler & Gordon, 2002), or other practices of e-commerce (Olivero & Lunt, 2004).

Van Dijk (2012) notes that people must reveal personal information in their OSN-profiles in order to be effective, and "teenagers and adolescents just have to do this to sound out their maturing identities" (p. 185). Communication on the internet can lead to more disclosure compared to face-to-face communication (Joinson & Paine, 2007). Beldad *et al.* (2011) argue that the personal information-related behavior of people can be conceptualized as a continuum. The authors describe this continuum as "information privacy protection behaviors such as information withholding and incomplete and inaccurate disclosure on one side, and complete and accurate information disclosure behaviors on the other." (p. 227). On OSNs this means that

users can still participate all whilst attempting to protect their personal information by only partly disclosing personal information.

Krasnova *et al.* (2010) note that a typical method to express disclosure is in terms of the breadth (amount of disclosed information) and depth (degree of intimacy) of the revelations a user makes. Depth, however, is highly subjective and too context-dependent. This makes the depth of disclosure very difficult to value (Joinson & Paine, 2007). In addition, note that "the economic value of a platform is not defined by how intimate users' revelations are, but rather by their participation, interaction and willingness to present themselves" (Krasnova, Hildebrand, Günther, Kovrigin & Nowobilska, 2008, as cited by Krasnova *et al.*, 2010). Therefore, this study is interested in the amount of disclosed information, not in the depth of this information.

In order to find answers to the first research question, these different factors that affect the disclosure will be explored in the following part of the report. It is also important to note that Youn (2005) found that "withholding true information appeared to be an important way of coping, which allowed teenagers to take part in online consumption without losing their privacy" (p. 104), and that teenagers were likely to falsify information if their motivation to protect their privacy increases. Metzger (2004) found that, although findings were inconsistent in literature, participants "tended to give inaccurate information for the items that were rated as more private". This falsification of information can be seen as incorrect 'data about the self', which is contrary to the operationalization of personal information and thus has to be taken into account.

2.2 Habits

Researchers are calling for the inclusion of habits in future research on OSNs (e.g. Cheung & Lee, 2010, p. 28) and the influence of habits in personal information sharing on OSNs is occasionally mentioned in recent literature (e.g. Davis & James, 2012; Beldad *et al.*, 2011; Van Dijk, 2012, p. 224). However, not much research has been conducted that focuses on the influence of habits on information disclosure in OSNs.

Habits can be defined as a recurrent behavior that does not require deliberate processing and instead results from automatic processing of stimulus cues. Because this report concerns itself with the behavior of personal information disclosure, this report will operationalize habits as 'the recurrent disclosure of personal information that does not require deliberate processing and instead results from automatic processing of stimulus cues'.

Lankton, McKnight and Thatcher (2012) state that habits applies well to the use behavior of OSNs. They back this statement up by the findings of Limayem, Hirt and Cheung (2007), who state that college students' internet use is often habitual (p. 656), and by the findings of Ellison, Steinfield and Lampe (2007), who found that questions concerning habitual use were mostly answered above the mean for Facebook user. Using the *habit theory*, Lankton, McKnight and Thatcher (2012) explain a relationship between habits and continuance intention. They state that habits can trigger intention automatically (Ajzan, 2002, p. 119) and a user can create even more amicable feelings towards certain behavior based on previous habitual activities. This increases the intention to continue this behavior, based on these habits (Ellison, Steinfield & Lampe, 2007).

Beldad *et al.* (2011) state that the benefits derived from disclosing information are not the only reason people share information, but also for the 'taste' of the disclosure itself (p. 226). The possible strong influence of habitual use is backed up by findings of Strater and Richter (2007), who found that some of their respondents were not sure why they shared information (p. 2). Others did not think twice when they supplied personal information when asked, just because they got used to filling out forms. Based on the findings above, it is hypothesized that:

H1: There is a positive casual relationship between an individuals' habits of disclosing personal information on OSNs and the intention to disclose personal information on OSNs.

In their article about reflections on past behavior, Verplanken and Orbell (2003) suggest the 'self-report habit index'. The authors suggest to break the concept of habits into "components that seem relatively easy to reflect on, such as the fact that habitual behavior is repetitive, difficult to control, goes with a lack of awareness, is efficient and may reflect one's identity." (p. 1325).

2.3 Benefits

Literature on the benefits of disclosure often conceptualizes the benefits in a 'risk versus reward' calculation. This might be the results of the *Social Exchange Theory* (which is often seen as the theoretical foundation of personal information disclosure), that states that interpersonal relationships are based on a subjective evaluation of benefits and costs (Homans, 1958, p. 606). The *Privacy Calculus Theory* argues that some users feel that the returns for disclosure offset the risk of their privacy being compromised (e.g. Dinev & Hart, 2006; Culnan & Armstrong, 1999).

Research found that people are willing to sacrifice the safety of their personal information if the perceived benefits outweighs the costs (for an overview, see Beldad et al, 2011, p. 225), and despite concerns about privacy, adolescents are particularly receptive to the potential benefits of disclosing personal information (Christofides, Muise & Desmarais, 2009, p. 342).

Benefits that are associated with disclosure are plentiful: enjoyment (e.g. Krasnova *et al.*, 2009); self-presentation (e.g. Boyd, 2009) and the opportunity to present only favorable information (e.g. Ellison, Heino & Gibbs, 2006); the ability to maintain social ties (e.g. Ellison, Steinfield & Lampe, 2007); displaying social capital to look important or popular (e.g. Christofides *et al.*, 2009; O'Murchu, Breslin & Decker, 2004); providing selective information to present oneself in a positive light or to be seen in a certain way (e.g. De Souza & Dick, 2009; Donath & Boyd, 2004); the enhanced possibilities for reciprocation (Krasnova *et al.*, 2010); and time saving or convenience (e.g. Hui, Tan & Goh, 2006; Hann, Hui, Lee & Png, 2007). Considering the vast amount of literature on the influence of benefits, it is hypothesized that:

H2: There is a positive causal relationship between personal benefits of disclosing personal information on OSNs and the intention to disclose personal information on OSNs.

2.4 Privacy and Perceived Privacy Risks

Privacy is a multifaceted concept (Beldad *et al.*, 2011), and this results in a multitude of definitions and concepts. A widely accepted view of privacy is "the individual's right to be left alone" (Warren & Brandeis, 1890). There has not been a consensus about the definition of privacy (Newell, 1995), stating that "perspectives on privacy are thus varied, occasionally conflicting, and generally difficult to evaluate in a coherent fashion" (p. 87). Privacy has been described as an 'umbrella term' for a wide and diverging group of related concepts (Solove, 2006, p. 486). Clarke (2006) and DeCew (1997) attempt to solve the problem of the umbrella term by proposing different dimension of privacy. Based on these two authors, Van Dijk (2012) proposes three dimensions: the right to selective intimacy; the right to select contacts without observation and intrusion; and the right to selective disclosure.

The third (Beldad *et al.*, 2011) and second dimensions are particularly salient in OSN environments. Gross & Acquisti (2005) confirm this, by stating that "in certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers[.]" (p. 72), which illustrates the importance of the third and fourth dimension of privacy in the OSN environment.

Dinev and Hart (2004) note that as in most empirical studies, the construct they aim to measure is operationalized indirectly rather than directly. For this report the attitude towards privacy of the person using disclosing personal information is what matters. And because this report concerns itself with disclosure of personal information, the term privacy predominantly entails 'personal information privacy'. In this report, private information is conceptualized as

'information that is selectively disclosed, and of which the sender has the right to select the recipients, without observation and intrusion of others'.

In line with the approach of Youn (2009) and Dinev & Hart (2004), this report is not primarily interested in the risks which the users of OSNs are aware of, but instead aims to explore and measure the perceived negative consequences that could result from information disclosure. For this reason, perceived risks is conceptualized as 'the perceived negative consequences that could happen to an individual as a result from disclosing personal information'.

Beldad *et al.* (2011, p. 222) note that the risks that are related to personal information disclosure are plentiful and that the risks depend on the amount and type of information that is disclosed. Even though the risks that online information suffer are more ambiguous to individuals, they generally are aware of dangers of privacy invasions (e.g. Staksrud & Livingstone, 2009) and the risks of unauthorized access to data (e.g. Rezgui, Bouguettaya & Eltoweissy, 2003). People generally realize personal information online is often used for the sake of financial gain (e.g. Olivero & Lunt, 2004). The inadequate protection of data (e.g. Youn, 2005) is also a risk that leads to concerns. Finally, users of OSNs are getting increasingly aware that information they openly publish can be abused by crooks, stalkers, bullies, or even one's own friends (e.g. Staksrud & Livingstone, 2009; Saunders and Zucker, 1999).

Recent media coverage, combined with negative personal experience, are very likely to further change users' perceptions of privacy threats (Smith, Milberg & Burke, 1996, p. 186). Individuals who disclose information online are often aware of the real-world consequences of their actions, because of the risk being identified online (Lee, Im & Taylor, 2008; Youn, 2005). This could explain why individuals' confidence of disclosure lessens when the sensitivity of the requested information increases (Castañeda & Montoro, 2007). Research also found that users often do not consider the full risks of information they disclose (Dwyer, 2007; Govani & Pashley, 2005).

Youn (2005) found that "as teens perceived privacy risks to be more severe, they were less likely to provide their personal information to a website". In a study on OSN-use by Qian and Scott (2007) half of all users choose to restrict full disclosure because of the associated perceived risks. Metzger (2004) found that internet users' concern for their online privacy negatively influences their online information disclosure. Malhotra, Kim, and Agarwal (2004) found evidence of a strong influence of perceived privacy risks on an individuals' behavioral intentions.

Even though there are conflicting findings about the influence of perceived privacy risks in personal information disclosure, the context, experiences, and recent developments in individuals' awareness of risks, it can be hypothesize that:

H3: There is a negative casual relationship between an individuals' perceived privacy risks of disclosing personal information on OSNs and the intention to disclose personal information on OSNs.

2.5 Privacy Valuation

Perceived privacy risks, or privacy concerns, are not necessary an indication of a individual's stance on the importance of their privacy. This is an important distinction, because the perceived privacy risks of disclosing personal information can change without a change in the personal privacy values of an individual.

Therefore, the choice is made to not just look at privacy as (a set of) privacy concerns —which do not necessary represent the values and attitude of the individual— but develop a separate construct called 'privacy valuation'. Although recent literature describes privacy valuation mostly as a tangible value or price to give up privacy (e.g. Acquisti, John & Loewenstein, 2009), this report operationalizes privacy valuation as 'an individual's attitude towards, and values about, personal information privacy'.

Westin (2003) notes the importance of personal values, or ideological interests, as an antecedent for perceived privacy risks. Every individual has different levels of concerns, or perceived risks, about his or her own privacy (Ackerman, Carnor & Reagle, 1999; Sheehan,

2002), and this is "based on that person's own perceptions and values" (Joinson & Paine, 2007, p. 244). This leads us to hypothesize that:

H4: There is a positive casual relationship between an individuals' privacy valuation of personal information shared on OSNs and the perceived privacy risks of disclosing personal information on OSNs.

However, the items used by Westin only offer the possibility to segment individuals into different categories, and offer no not continuous (or quantitative) results. Therefore, his proposed items are not suitable for this research and need adjustments to be useable for this research.

2.6 Trust

Generally, trust is defined as the willingness of a 'truster' to be vulnerable to the actions of a 'trustee', based on the expectation that the trustee will perform a particular action important to the truster, regardless of the ability to monitor or control the trustee (Schoorman, Mayer & Davis, 2007). McKnight, Choudhury, and Kacmar (2002) state that there are three antecedents to trusting behavioral intentions and each of these antecedents consists out of three factors: competence (or ability), benevolence, and integrity.

A fitting operationalization for trust for this report is one by Dinev and Hart (2006), who define trust as "the beliefs reflecting confidence that personal information submitted to internet websites will be handled competently, reliably, and safely." (p. 64).

In the context of OSNs, there is no consensus in current literature about the relationship between trust and perceived privacy risks (Krasnova *et al.*, 2010). Gefen *et al.* (2003) note that, in situations where risk is inherent to an action, trust will reduce the risks that are perceived. Risk will, in turn, directly influence behavior. Kim *et al.* (2008) support this claim and argue that, when an activity is perceived as risky and an individual does not have full control over the outcome, the importance of trust increases. In addition, Krasnova *et al.* (2010, p. 114) state that "trusting beliefs mitigate risk perceptions".

The presence of security mechanisms significantly increases trust in online exchanges (Beldad et al., 2011, p. 225). Websites like Facebook offer a set of security mechanisms (ranging from extra steps of authentication when logging in to secure connections when browsing the site), a very extensive privacy statement, and multiple tools to check your privacy and security settings. Therefore it is hypothesized that:

H5a: There is a positive causal relationship between an individuals' trust in the parties the personal information is shared with and the perceived privacy risks of disclosing personal information on OSNs.

Trust is important for successful online interactions overall (Dwyer, Hiltz & Passerini, 2007). As shown in previous research, trust and self-disclosure have a reciprocal relationship in online communication (Henderson & Gilding, 2004). Multiple authors found support for the claim that internet users' trust positively influenced their information disclosure (e.g. Metzger, 2004; Fogel & Nehmad, 2009; Mesch, 2012).

In addition, Taddei and Contena (2013, p. 822) state that "users with a high level of trust are more comfortable with intimate topics and so they disclose more personal information". Based on these findings, it is hypothesized that:

H5b: There is a positive causal relationship between an individuals' trust in the parties the personal information is shared with and the intention to disclose personal information on OSNs.

2.7 Perceived Control

In his *Comprehensive Interpretation of Privacy* Clarke (2006) notes the importance of control over personal information: "Information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." (p. 5). The concept of control is also salient in Westin's (1967) definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (p. 7, as cited in Beldad *et al.*, 2011). A number of other definitions of privacy also mention the importance of control in information privacy (see Beldad *et al.*, 2011, p. 221).

Because this report concerns personal information disclosure, control will refer to control over personal information. For this report 'perceived control' will be operationalized 'the power to influence or direct personal information by selective disclosure and the right to select contacts without observation and intrusion'. This definition is based on both the standard definition of control by Augarde (1981) and Van Dijk (2012).

Beldad *et al.* (2011) argue that "when individuals have control over information dissemination and information access, they have acquired a certain level of information privacy". Dinev and Hart (2003) concluded in their research that when companies grant consumers control over their information, the consumers develops a more trusting attitude. Das and Teng (1998) also argue that control is an important way to create trust and confidence in cooperative behavior between parties.

Krasnova *et al.* (2010) state that, if individuals are given the right tools on OSNs to manage their privacy management, they are more likely to gain trust in other members. To manage their privacy, websites like Facebook allow its users to change personal settings to control who can access and view which information on their profile (Waters & Ackerman, 2011). Taddei and Contena (2013) found that on OSNs the perceived control directly influences the perception of trust. Therefore it is hypothesized that:

H6a: There is a positive causal relationship between an individuals' perceived control over personal information shared on OSNs and their trust in the parties the personal information is shared with.

Consumers do not find it acceptable when personal information is being collected without their consent or that marketeers sell their personal information (Dinev & Hart, 2004; Milne, 2000; Cespedes & Smith, 2012). Internet users are becoming increasingly aware of the power of internet technologies to monitor user behavior, and more individuals realize that service providers gather information about them without their knowledge (Dinev & Hart, 2004).

Youn (2009) concluded that, among young adolescents, the level of perceived privacy risks motivates coping behaviors to handle these privacy risks. Dinev and Hart (2004) found that a perceived vulnerability to privacy risks was positively related to perceived privacy risks. In addition, they mention that the ability to control personal information is seen as a separate construct from perceived privacy risks, but that these two constructs are related.

Culnan and Armstrong (1999) underscore the role of control in risk reduction by arguing that letting consumers be in charge of their personal information can be seen as a pre-condition to lower their perception of privacy risks and improve their trust. Krasnova *et al.* (2010) state that by offering users (at least some) control over their privacy settings, OSN providers can empower their users.

Xu, Dinev, Smith and Hart (2008) empirically demonstrated that providing mechanisms to exercise self-controlling are important to diminish the perceived privacy risk on OSNs. Websites like Facebook offer a set of possibilities and settings to control the users' personal information. Therefore, it is hypothesized that:

H6b: There is a negative causal relationship between an individuals' perceived control over personal information shared on OSNs and the perceived privacy risks of disclosing personal information on OSNs.

When control over personal information is not permitted by a service provider, or when the future use of the information is unknown, people resist to disclose (Dinev & Hart, 2004). When looking at online interaction and communication, Culnan and Armstrong (1999) state that empowering the users with control over their information is especially important, as there is a significant social distance between participants.

Krasnova *et al.* (2010) conclude that, when there is no certainty about the incentives of the (OSN) service provider due to restricted control over the information, it results in restricted disclosure. As a result of the perceived negative attention associated with this restricted control, individuals inflate the risks they associate with disclosure, which causes them to disclose less information. This leads to the following hypothesis:

H6c: There is a positive causal relationship between an individuals' perceived control over personal information shared on OSNs and the intention to disclose personal information on OSNs.

The aforementioned nine hypotheses and two research subquestions are presented in a research model (see Figure 1).

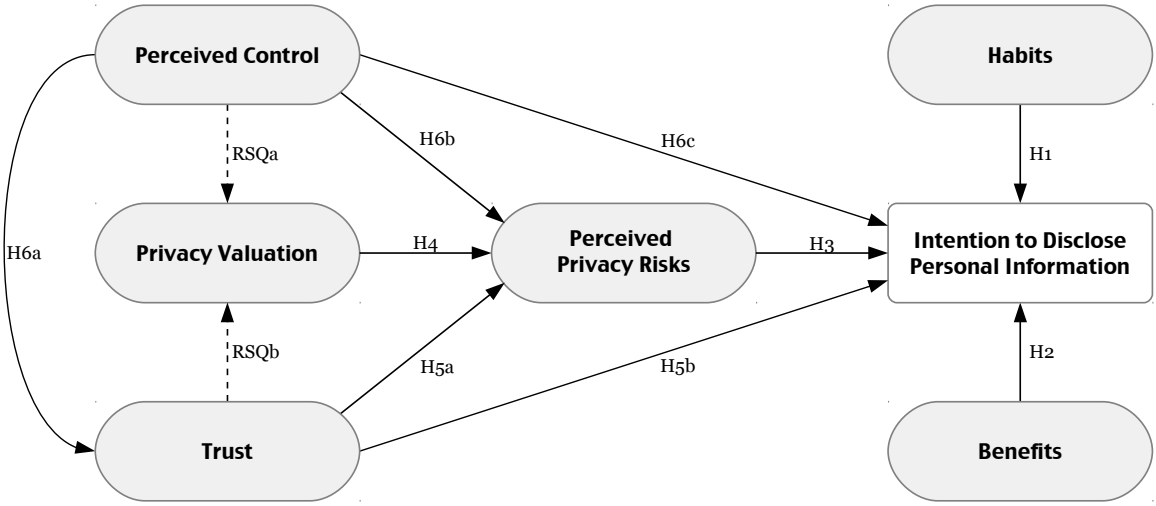


Figure 1: Research model of disclosing personal information on online social networks.

2.8 Demographics and Facebook Usage

Even though the research questions do not concern demographics (e.g. gender, age, or education) or the variables that cover the use of Facebook without disclosing personal information (e.g. frequency of visits, average duration of visits, or amount of Facebook friends), literature shows that gender (e.g. Fogel & Nehmad, 2009, p. 154; Tufekci, 2008), education (e.g. Youn, 2009, p. 390; De Souza & Dick, 2009, p. 260), or age (e.g. Hinduja & Patchin, 2008; Tufekci, 2008) can have an influence on disclosure. To be able to isolate the possible unequal distributed influence of these variables, they need to be measured.

3 Research Method

This chapter will discuss the setup of the empirical study. First, it is explained why Facebook[1] is used to explore the research questions and test the hypotheses about personal information disclosure on online social networks, and the choice to conduct the research with (young) adolescents who are currently in high school will be discussed.

The second part of this chapter discusses the research tool, and explains the development of the items per variable. It is important to note that this chapters also provides a thorough explanation on the measurement of *social desirable responses*. In addition, it discusses the means to measure these responses that are potentially harmful to the integrity and validity of a research that relies on self-reporting.

3.1 Choice of OSN and respondents

Facebook is a well-known online social networking service and was founded in 2004, initially limited to Harvard students. In 2006, Facebook opened up for everyone with the mission statement "to give people the power to share and make the world more open and connected" (Facebook.com, 2013). Facebook has 1.11 billion monthly active users, with an average of 655 million users who are active on a daily basis, and 751 million users visit Facebook on a mobile device each month (Facebook.com, 2013). In the Netherlands 83% of internet users between 16 and 35 years old use Facebook (Van Deursen & Van Dijk, 2012).

Facebook offers a very wide range of services. The website primarily resolves around the 'news feed', which gives an overview of information you or your contacts shared. Each personal profile has a 'timeline', or a 'wall'. This gives a chronological overview of all the information about the person that is ever shared. This can be anything from messages, pictures, videos, 'pokes', 'likes', or 'tags' of places or other contacts. The most prominent contact on Facebook is a 'Friend'. In this report, the term 'friend' is used to indicate a consensual connection between two users on Facebook. You can send personal messages or chat with your direct friends. You can set up groups, events, or 'pages' to interact with specific audiences without having to befriend them on the website.

Because of the popularity, reach, unique properties, completeness of provided services, and complexity and depth that Facebook offers to their users, this research will aim to answer the research questions using Facebook as a representation of other OSNs.

(Young) Adolescents on OSNs

Since the rapid increasing popularity of OSNs, the information disclosure of young adolescents on these services has intensified worries about loss of privacy (e.g. Livingstone, 2008; Lenhart & Madden, 2007; Romer, 2006).

In response to these concerns researchers started to empirically research adolescents and their attitudes toward online privacy concerns (e.g Grant, 2005, 2006; Youn, 2005, 2008; Moscardelli & Divine, 2007). But for teens the need to be a part of a social group and to be popular are important parts of their lives (Santor, Messervey & Kusumakar, 2000). This can explain why teens have a strong presence and visibility on OSNs, and (Boyd, 2009). Youn (2005) found that while numerous studies have examined the privacy concerns and coping behaviors of older (ranging from the age of 14 to 18) adolescents', there is little known about how younger (ranging from the age of 11 to 13) adolescents perceive online privacy and how they respond to their privacy concerns.

Yan (2006) states that "children have reached the adult level of understanding the technical complexity of the internet" (p. 426) at 12 years old. However, it is not until early adolescence (age 13 to 14) before "children reach the adult level of understanding the social complexity of the internet" (p. 426). Facebook prohibits people who are younger than 13 to sign up. This does not stop younger teens from falsifying the information about their age and signing up for an account

[1] *Throughout this article Facebook refers to the online social network service, available at http://www.facebook.com*

if they'd want to. According to *Consumer Reports* (2011) there are at least 7.5 million children under 13 with accounts. If Yan's (2006) findings are correct, young adolescents will provide results that are comparable to those of adults.

Based on these findings the choice is made to conduct the empirical research with this age-group. Out of convenience, the research will be conducted at a high school in the Twente, The Netherlands. This school knows seven educational departments, ranging from *BBL* (practical) to *Gymnasium (*pre-university) education. In school year 2011-2012 the school had around 1300 students, ranging from twelve to eighteen years old.

3.2 Development of Measurement Scales

All items are to be rated on a 5-point *Likert-Scale*, ranging from 1 — 'Strongly Agree' to 5 — 'Strongly Disagree', unless stated otherwise.

Intention to Disclose Personal Information

In order to measure disclosure as it is operationalized in this report, the possible means of disclosure Facebook offers to its users are important. Next, the questionnaire should aim to measure how often and how much they make any form of information shared knowledge. The items *DPI9* to *DPI15* (see Appendix A, Table 1) aim to answer this question.

It is necessary to exclude the possibility that respondents share bogus data, because falsified information is not 'information about the self'. The items *DPI1* to *DPI8* (see Appendix A, Table 1) were designed to check for this concern, and provide the option to answer 'No', 'Yes, but the info is incorrect', or 'Yes, and the info is correct' to questions about certain pieces of information the respondents can share on their personal Facebook-profile.

Habits

In order to measure habits, items suggested by Verplanken and Orbell (2003) were modified in such a way they reflect habits in information disclosure, and not use of the site (see items *Hab5* to *Hab8*, Appendix A, Table 1).

Benefits

To measure the benefits, the items suggested by Krasnova *et al.* (2010, p. 117) and Ellison, Heino, and Gibbs (2007, p. 1151) were used. However, both articles formulated the questions in such a way they cover OSN use, and not information disclosure per se (e.g. "I get to know new people through the OSN" instead of 'I get to know new people by sharing personal information on the OSN' or "I try to make a good impression on others on the OSN" instead of 'I try to make a good impression on other by sharing personal information on the OSN'). As a results, the items risk that they do not measure what they intended to measure. Therefore, the questions were adjusted to be more fitting for Facebook (see items *Ben1* to *Ben8*, Appendix A, Table 1).

Perceived Privacy Risks

Dinev and Hart (2004) suggested four items items that measure privacy concerns. However, these items do not make a distinction between the *risk-targets* (the different parties the personal information is disclosed with). Therefore, the proposed items were adjusted to measure the perceived privacy risks as a result of disclosing with Facebook and other parties that are not the respondents' friends (see items *PPR1* to *PPR5*, Appendix A, Table 1), the individuals' friends (*PPR6* to *PPR8*) and one's own influence (*PPR9* to *PPR11*). It should be noted that some parties, especially for items *PPR1* to *PPR5*, can be unknown to an individual, but still have some risk attached to it (i.e. hackers, marketeers).

Privacy Valuation

In this report privacy valuation is operationalized as an individual's attitude towards, and values about, personal information privacy. Because no recent literature was found that could provide

items that were suitable to test the variable as it is operationalized in this report, a set of items suggested by Dr. Ardion Beldad[2] in an unpublished research-paper was used (see items *PrV1* to *PrV4*, Appendix A, Table 1).

Trust

As with the variable 'perceived privacy risks', this variable can have different targets. The items suggested by Krasnova *et al.* (2010, p. 117) were adjusted to be more fitting for Facebook, while making the distinction between trust in Facebook as a company (see items *Tru1*, *Tru2*, *Tru6*, and *Tru7*, Appendix A, Table 1), and trust in Facebook-friends (see items *Tru3* to *Tru5*).

Contrary to the items for 'perceived privacy risks', the items for this variable do not aim to measure trust in, for instance, friends-of-friends or other unknown parties. The reasoning behind this is that these parties are either unknown to an individual, or too abstract, to found one's trusting beliefs on.

Perceived Control

As mentioned before, the respondents have the possibility to exert control by using the privacy and security settings that Facebook offer to their users. Krasnova *et al.* (2010, p. 117) suggested three items, which were adjusted to be more fitting to Facebook. In addition, two items were added (see items *PeC1* to *PeC5*, Appendix A), with the goal to measure the perceived power to influence or direct personal information by selective disclosure using the provided Facebook-settings.

Social Desirability

'Socially desirable responding' (*SDR*) is the tendency for participants to present a favorable image of themselves (Johnson & Fendrich, 2005) and confounds the results of a research by obscuring or creating false relationships between variables. Participant can actually believe the information they report (self-deception) or they 'fake good' to conform to socially acceptable values, avoid criticism, or gain social approval (King & Brunner, 2000; Huang, Liao & Chang, 1998). Although socially desirable responding is most likely to occur in responses to socially sensitive questions (King & Brunner, 2000) like dietary intake, domestic violence, and sexual practices, the SDR bias affects the validity of any questionnaire (Huang, Liao & Chang, 1998). Researchers claim that between 10% to as much as 75% of the variance in participants' responses can be explained by SDR (Nederhof, 1985).

Social desirability scales can be used to detect, minimize, and correct for SDR in order to improve the validity of questionnaire-based research (Van de Mortel, 2008). The most widely used and tested scale is the 33-item *Marlowe-Crowne Social Desirability Scale* (MCSDS), but other shorter versions have been validated as well (Reynolds, 1982; Ballard, 1992). People who score high on these scales have a high need for social approval and are more likely to portray themselves positively and visa versa (King & Brunner, 2000). According to Edens, Buffington, Tominic and Riley (2001, p.249) there is no "categorical standard for differentiating between socially desirable and non-socially desirable responding". The authors suggested that a participant who scored 1.5 standard deviations or more above the mean for the sample could be labeled as a 'high scorer'.

Because of the possible influence of SDR, the choice is made use of *M-C Form A* as defined by Reynolds (1982). This version uses 11 items that need to be answered as either 'Not true' or 'True', and demonstrates an acceptable level of reliability (Reynold, 1982, p. 123) while having the advantage of being considerably shorter (see items *SoD1* to *SoD11*, Appendix A, Table 1).

---

[2] *Correspondence: A. Beldad. Department of Communication Science - Corporate and Marketing Communication, University of Twente, 7500AE Enschede, The Netherlands. Tel: (+31)53 489 2322 E-mail: a.d.beldad@utwente.nl*

Demographics, Frequency and Duration of Visits, Account Age, and Number of Friends

The item about gender and the item about the educational level are categorical, and the item about the age can scale from 11 to 18 years (see items *Dem1* to *Dem3*, Appendix A, Table 1). To maintain consistency, the questionnaire has to be filled out by every student, whether they have, had, or never had an Facebook-account (see item *Dem4*, Appendix A, Table 1).

Information on how often and how long individuals visit Facebook, how long they have an account, and how many Facebook-friends they have (see items *Hab1* to *Hab4*, Appendix A, Table 1) need to be collected. The first two items about 'habits' are categorical, and the other two are on a numerical scale. Even though these are not necessarily indications of habits in information sharing, this information provide a context that is necessary to value the items about habitual disclosure.

3.3 Pre-test and Distribution of the Questionnaire

Because there is a big difference in level of education and age in the pool of respondents, a pre-test with 19 students has been conducted to make sure the language was comprehendible. Nine students (ranging from 12 year old *VMBO* to 16 year old *VWO*) filled out the questionnaire and were asked for feedback, and ten students were orally questioned on their own and classmates' Facebook-use.

The result from the students who filled out the questionnaire were positive. The questionnaire was comprehendible for all volunteering students, and all students were able to finish the questionnaire within 11 minutes. The wording of two items were slightly adjusted to avoid confusion, and one item about the use of the 'Facebook-chat' was added (see Appendix A, Table 1, item *DPI15*).

From the oral sampling it appeared that fewer students than anticipated had an active Facebook-account. Students from the first and second grade guessed that 6 to 12 students (from a class of about 25 students) had a Facebook-account. Older students appear to be substantially more active on Facebook, and guessed that 15 to 20 out of 25 classmates had an account. To make sure the research would end up with enough useable data (i.e., student who have a Facebook-account and use it), the school-board gave a green light to distribute the questionnaire to more students.

The questionnaires were distributed by the teacher at the start of the class. Students were informed not to talk or discuss the answers with each other, and hand over the questionnaires if they were finished. The Dutch version, that has been handed out to the respondents, can be found in Appendix B.

4 Results

A total of 921 questionnaires were collected between April 11th and April 25th 2013. After removing the incomplete or otherwise unusable questionnaires, the 855 questionnaires (resulting in a 92.8% response rate) were entered in *IBM SPSS Statistics 21*. From this sample, 26.3% (n = 225) never had a Facebook-account, and 8.2% (n = 70) used to have a Facebook-account, but did not have one anymore. This resulted in 570 questionnaires suitable for further analysis.

4.1 Social Desirable Responding

Before the data was used in further analyses, it had to be tested wether or not a part of the variance in the data could be accounted to the influence of SDR. The results of the SDR-scores for the 570 respondents are presented in Figure 2.

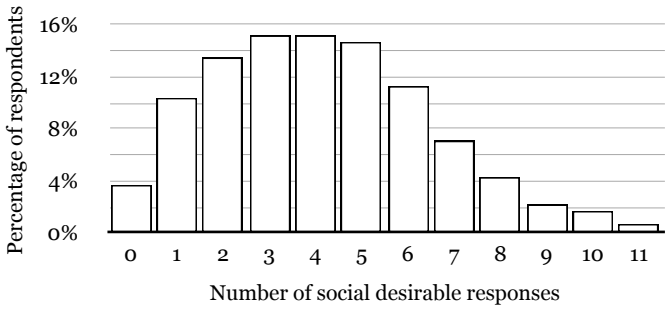


Figure 2: SDR-score distribution

With a *skewness* score of .44 and a *Kurtosis* score of -.22 the SDR-scores are approximately symmetrical and normally distributed (Bulmer, 1979, p. 63). In this sample, where the scores could range from 0 to 11, males were more inclined to give socially desirable answers (M = 4.72, SD = 2.45) compared to females (M = 3.63, SD = 2.20). There was no significant difference in SDR scores between the different age groups or educational levels.

As mentioned before, there is no categorical standard for differentiating between socially desirable and non-socially desirable responding. Edens *et al.* (2001, p. 249) suggest that a participant who scored 1.5 standard deviations or more above the mean for the sample could be labeled as a 'high scorer' (in this case 8 questions or more). In order to check if there are significant differences between SDR respondents (i.e. 'high scorer') and non-SDR respondents, the mean and standard deviation of the seven different variables (Table 1) are compared.

Table 1
Comparison of Social Desirable Responses scores for all variables

	All responses (N=570)		Non SDR (n=491)		SDR (n=79)		SDR vs. non-SDR	
Variable	Mean	SD	Mean	SD	Mean	SD	Diff. in Mean	Diff. in SD
Disclosure	2.55	0.84	2.57	0.83	2.56	0.87	-0.01	0.04
Trust	3.66	0.74	3.68	0.72	3.47	0.87	-0.21	0.15
Privacy Risks	2.45	0.63	2.44	0.64	2.57	0.58	0.14	-0.06
Benefits	2.58	0.68	2.57	0.69	2.78	0.55	0.21	-0.14
Privacy Valuation	4.31	0.73	4.34	0.73	3.98	0.78	-0.35	0.06
Control	3.97	0.79	3.99	0.80	3.83	0.75	-0.16	-0.05
Habits	2.18	0.83	2.17	0.82	2.36	0.86	0.19	0.04

Note. The value of the variables' mean could range from 1 to 5.

The biggest difference in the mean was found in the questions about 'privacy valuation'; the mean for this variable is 0.35 points lower for individuals who are prone to give socially desirable answers, which is almost half of a standard deviation. However, the most important observation in Table 1 is that the influence of SDR is not unidirectional. It was hypothesized that, for instance, 'perceived control' and 'habits' both have a positive causal relation with 'intention to disclose personal information'. And while items about disclosure were pretty much unaffected, SDR had a negative influence on items about 'perceived control' but a positive influence on items about 'habits' (with a discrepancy between both means of 0.35).

Because the influence of SDR does not appear to be unidirectional, the 79 high-scorers (13.9% of the total of 570 respondents) were excluded in the remaining statistical analyses.

4.2 Demographics and Facebook Use

After removal of the SDR 'high-scorers' there was a total of 491 usable observations left, with 44.4% (n = 218) male and 55.6% (n = 273) female respondents. Close to 88% of the respondent with a Facebook-account were 13 to 16 years old, and 7.7% (n = 38) were 12 years old. Interestingly enough, only slightly more than half (55.3%) of this youngest group answered the item "I filled in my date of birth." with the only possible correct answer ('Yes, but the info is incorrect.').

Table 2
Respondents' educational level, distributed by school-year.

	Bovenbouw				Onderbouw		
School-year	BBL	VMBO	Havo/ VWO	VWO+	Havo	VWO	Gymna-sium
1 (n=94)	5 (5%)	41 (44%)	42 (45%)	6 (6%)	-	-	-
2 (n=105)	11 (10%)	27 (25%)	54 (51%)	13 (12%)	-	-	-
3 (n=126)	-	-	-	-	73 (58%)	34 (27%)	19 (15%)
4 (n=166)	-	-	-	-	115 (69%)	51 (31%)	0 (0%)

*Note. Dutch high-schools have two levels (*onderbouw *roughly translates to 'substructure' and* bovenbouw *to 'upperstructure'), each with different levels of education.* BBL *is practical education,* VMBO *is preparatory profession education,* HAVO *could be translated as general secondary school, and* VWO *is pre-university education.* VWO+ *is an early preparation for research-oriented education, and* Gymnasium *is equal to* VWO*, but with additional mandatory courses.*

On average the Facebook-account of respondents was over 20 months old (M = 20.32, SD = 12.64) and the respondent had an average of 189 friends (SD = 144.70). Even though the respondents were asked to guess their approximate number of friends, 67 individuals did not provide an answer to this question, indicating more often than not they "did not have a clue".

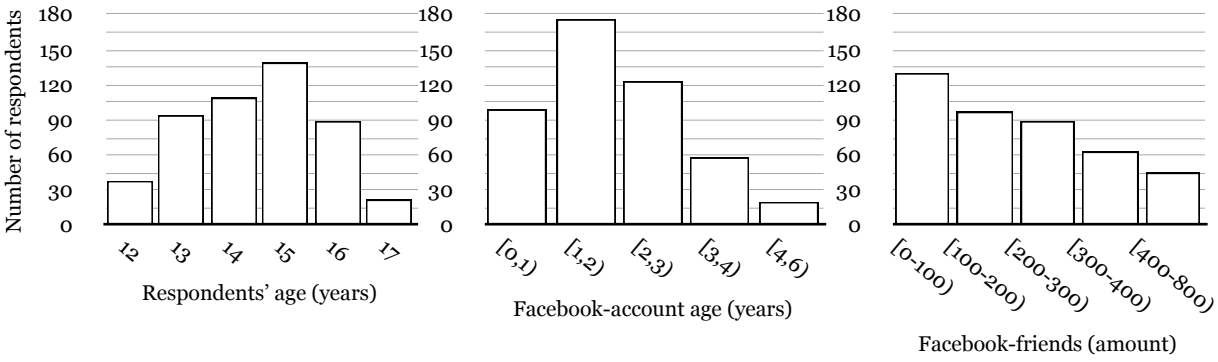


Figure 3: Distribution of respondents' age (left), Facebook-account age (middle), and number of Facebook-friends (right).

Only 8.2% of the respondents said they visited Facebook 'More than 10 times a day', 11% answered 'Five to ten times a day', most respondents visited Facebook 'Once to five times a day' (36.5%), followed by 'A few times a week' (26.5%), and finally 17.8% said they visited Facebook 'Once a week, or less'. The average 'Time spend per visit' was very close for the first four visit-frequencies ($2.58 < M < 2.70$), with 'One time or less a week' being the only outlier ($M = 1.98$). Both 'Facebook account age' and 'Number of Facebook-friends' appears to correlate with the respondents' frequency of use (for full details, see Appendix C, Table 2).

Figure 4 shows a comparison for the variables 'disclosure' and 'correctly provided Facebook-profile information', based on frequency of Facebook-visits. Frequent visitors appear to disclose personal information more often (left) and have a more comprehensive profile with more correct info (right), compared to respondents who indicated visit Facebook less often.

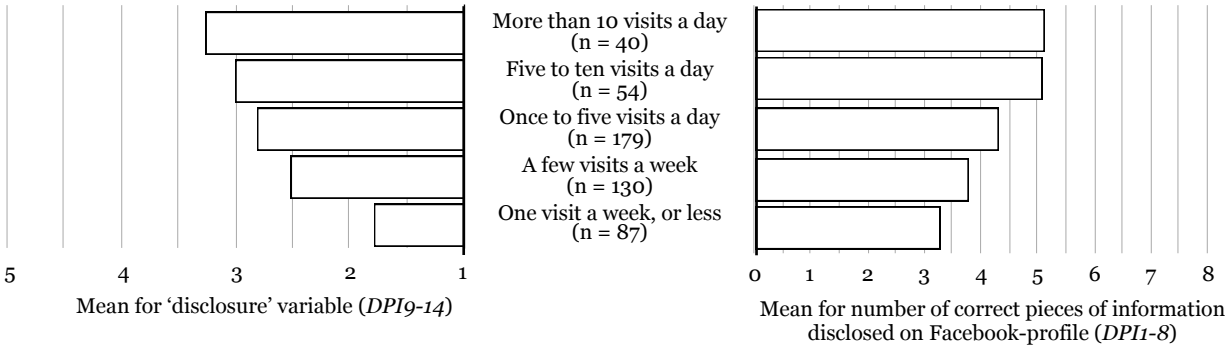


Figure 4: Comparison of means for 'disclosure' (left) and 'correctly provided Facebook-profile information' (right) based on frequency of Facebook-visits.

4.3 Falsifying Information

Respondents indicated they did not falsify information often; on average 1 in 27 pieces of information that was provided on the respondents' Facebook-profile was falsified. Respondents claimed that out of the 8 pieces of information, they provided an average of 4 correctly ($M = 4.15$, $SD = 1.53$), closely followed by not providing the requested information ($M = 3.53$, $SD = 1.36$).

Close to all of the respondents provided their correct first (97.1%) and last name (95.9%). The day of birth was falsified the most (16.3%), and respondents in the age group of 12 years old claimed to have falsified most information; out of the 4 pieces of information they provided on their profile on average, 1 was falsified. This is a big difference compared to the 17-year olds, where close to 1 out of 29 pieces of information was incorrect. The correlation between age and information disclosed on their profile is clearly visible in Figure 5; the age of the respondent appears to be the strongest indication for both providing correct information ($\beta = .38$, $p < 0.001$) and falsifying ($\beta = -.29$, $p < 0.001$) information. An statistical overview for information falsification per age group can be found in Appendix C, Table 3.

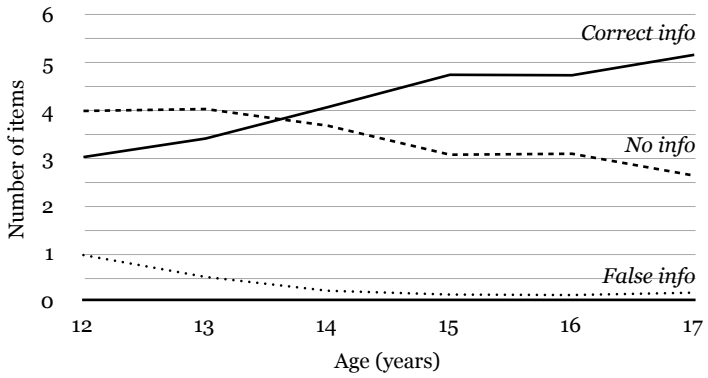


Figure 5: Comparison of number of items of information disclosed on the respondents' profile, by age.

4.4 Variable Composition, Statistics, and Reliability Analysis

With the results from the factor analysis, item sets were composed that had an as strong as possible internal consistency. By performing a reliability analysis on the individual sets of items that resulted from the factor analysis, items that damaged the reliability were removed as long as the removal of this item did not damage the integrity of the set of items as a whole.

The general rule of thumb is that a Cronbach's Alpha (α) of .90 or higher is excellent, an α from .90 to .80 is good, and and α from .80 to .70 is acceptable (Kline, 2000). Table 4 shows the Cronbach's Alphas for the ideal variable compositions. All constructs surpassed the recommended value ($\alpha > .70$). Thus, overall internal consistency can be assumed.

Table 4
Number of items, variable mean, standard deviation, and reliability of variables

Variable	Items	Mean	SD	α
Intention to Disclose Personal Information	5	2.61	0.86	.83
Trust	7	3.68	0.72	.84
Perceived Privacy Risks	7	2.24	0.77	.85
Benefits	8	2.57	0.69	.81
Privacy Valuation	4	4.34	0.73	.78
Perceived Control	3	4.12	0.92	.81
Habits	4	2.17	0.82	.73

Note. Appendix A, Table 1 shows the questionnaire-items that were used in the questionnaire. The value of the variables' mean could range from 1 to 5.

The variable's composition and the individual items' mean and standard deviation can be found in Appendix C, Table 1.

4.5 Correlation Analysis

Table 5 shows the correlation between the different variables. Even though correlation does not imply causation, correlations are useful because they can indicate a predictive relationship. These values will be further discussed in the *Discussion* chapter.

Table 5
Variable correlation

Variable	DPI	Tru	PPR	Ben	PrV	PeC	Hab
Intention to Disclose Personal Information (DPI)	*.75*						
Trust (Tru)	.18*	*.51*					
Perceived Privacy Risks (PPR)	.00	-.25*	*.59*				
Benefits (Ben)	.29*	.04	.27*	*.48*			
Privacy Valuation (PrV)	.16*	.45*	-.01	-.06	*.53*		
Perceived Control (PeC)	.27*	.33*	-.03	.01	.50*	*.85*	
Habits (Hab)	.44*	.01	.16*	.43*	-.22*	-.01	*.67*

*Note. * indicates a significance at the 0.001 level (1-tailed). The cursive values are the covariance-scores.*

4.6 Linear Regression Analysis

Linear regression was used to fit the predictive model to the observed data set. An overview of the variables and their corresponding predictors, coefficients, and significance are shown in Table 6a to Table 6d. The adjusted R^2 provides a measure of how well the observed outcomes are replicated by the model and explains the proportion of total variation of outcomes explained by the model.

Table 6a
Coefficients of the variables predicted to influence 'intention to disclose personal information'

Predictor	B	SE B	β	t	R	R^2 ($\triangle R^2$)
(Constant)	0.20	0.26		0.78	.53	.29 (.28)**
Trust	0.10	0.05	.08	1.90		
Perceived Control	0.23	0.04	.24 **	5.92		
Habits	0.43	0.05	.40 **	9.47		
Perceived Privacy Risks	-0.07	0.05	-.06	-1.49		
Benefits	0.14	0.06	.11 *	2.53		

*Note. ** indicates a significance at the 0.001 level, and * a significance at the 0.05 level.*

Table 6b
Coefficients of the variables predicted to influence 'perceived privacy risks'

Predictor	B	SE B	β	t	R	R^2 ($\triangle R^2$)
(Constant)	2.87	0.23		12.70	.28	.08 (.07)**
Trust	-0.33	0.05	-.31 **	-6.30		
Privacy Valuation	0.13	0.06	.12 *	2.23		
Perceived Control	0.01	0.04	.01	0.25		

*Note. ** indicates a significance at the 0.001 level, and * a significance at the 0.05 level.*

Table 6c
Coefficients of the variables predicted to influence 'privacy valuation'

Predictor	B	SE B	β	t	R	R^2 ($\triangle R^2$)
(Constant)	1.88	0.16		11.76	.58	.34 (.33)**
Trust	0.32	0.04	-.32 **	8.22		
Perceived Control	0.31	0.03	.39 **	9.97		

*Note. ** indicates a significance at the 0.001 level.*

Table 6d
Coefficients of the variable predicted to influence 'trust'

Predictor	B	SE B	β	t	R	R^2 ($\triangle R^2$)
(Constant)	2.62	0.14		18.62	.33	.11 (.11)**
Perceived Control	0.26	0.03	.33 **	7.73		

*Note. ** indicates a significance at the 0.001 level.*

Table 6a to 6d show that out of the 11 analyzed predictors, 6 tested as very significant ($p < 0.001$), 2 were significant ($p < 0.05$), and 3 predictors were not significant ($p > 0.05$). The variable 'habits' is the strongest predictor for the variable 'intention to disclose personal information' ($\beta = .40$), followed by 'perceived control' ($\beta = .24$) and 'benefits' ($\beta = .11$). It was found that 27.8% of the variance of 'intention to disclose personal information' could be explained by the 5 predictors 'perceived control', 'trust', 'benefits', 'perceived privacy risks', and

'habits'. Table 7 shows an overview of the hypotheses that were formulated to be able to answer the main research question.

Table 7
Overview of the hypotheses their corresponding results

Hyp.	Variable Relation	Result
H1	Habits $\xrightarrow{+}$ Intention to Disclose Personal Information	Supported
H2	Benefits $\xrightarrow{+}$ Intention to Disclose Personal Information	Supported
H3	Perceived Privacy Risks $\xrightarrow{-}$ Intention to Disclose Personal Information	Rejected
H4	Privacy Valuation $\xrightarrow{+}$ Perceived Privacy Risks	Supported
H5a	Trust $\xrightarrow{-}$ Perceived Privacy Risks	Supported
H5b	Trust $\xrightarrow{+}$ Intention to Disclose Personal Information	Rejected
H6a	Perceived Control $\xrightarrow{+}$ Trust	Supported
H6b	Perceived Control $\xrightarrow{-}$ Perceived Privacy Risks	Rejected
H6c	Perceived Control $\xrightarrow{+}$ Habits	Supported

The linear regression analyses also showed that there was a significant ($p < 0.001$) positive causal relationship between an individuals' 'perceived control' ($\beta = .39$) and 'privacy valuation' and 'trust' ($\beta = .32$) and 'privacy valuation'. These findings provide an answer to the research subquestion.

As mentioned before, the data supports 8 of the 11 tested relations. In addition, *Hypothesis 5b*, one of the three rejected hypotheses, was very close to being statistically significant ($p = .06$). Figure 6 shows the proposed model as presented in Figure 1, with the addition of the coefficients of determination values that resulted from the linear regression analyses.

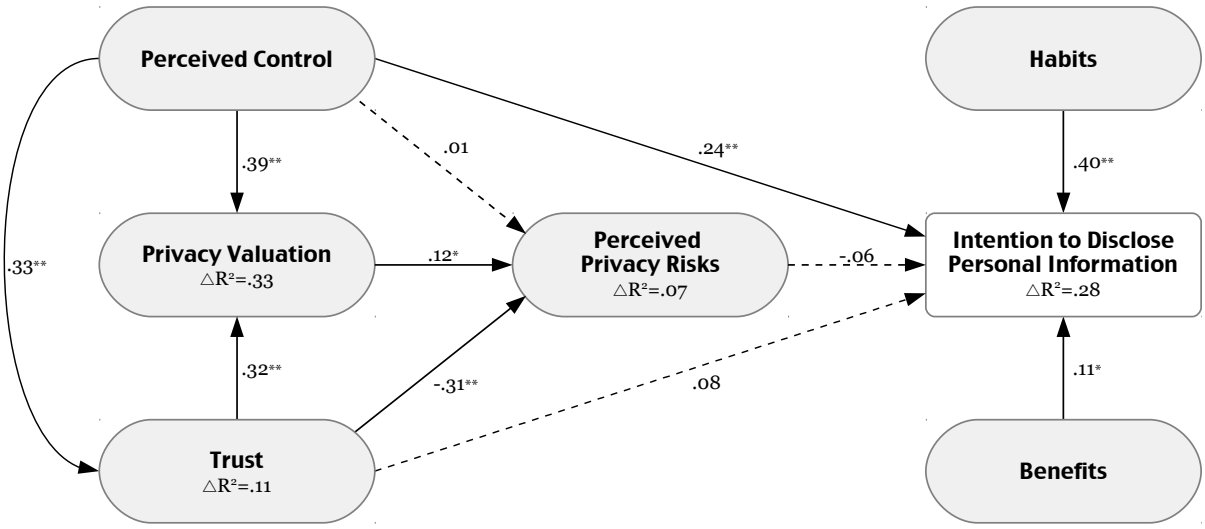


Figure 6: Results for the linear regression analyses. * indicates a significance at the 0.05 level, ** a significance at the 0.001 level . A dashed line represents an insignificant link.

In addition to the analyses that are required to answer the hypotheses, Table 8 shows the coefficients for 'intention to disclose personal information' with the predictors 'gender', 'age', 'frequency of visits', 'average duration of visits', 'account age', 'number of friends', and 'educational level' added to the six variables that were used in the original analysis. These variables are not a part of the proposed research question. However, even though the data was collected for other purposes, an additional linear regression analysis could provide interesting insights for future research or implications, because literature suggests that these factors can have a substantial influence on disclosing behavior.

Table 8
Coefficients of additional variables that influence 'intention to disclose personal information'

Predictor	B	SE B	β	t	R	R^2 ($\triangle R^2$)
(Constant)	.77	0.40		1.94	.72	.52 (.51)***
Trust	.02	0.04	.02	0.43		
Perceived Privacy Risks	-.06	0.04	-.05	-1.52		
Benefits	.11	0.05	.09 *	2.36		
Perceived Control	.13	0.03	.13 ***	3.88		
Habits	.34	0.04	.32 ***	9.03		
Gender	.43	0.06	.25 ***	7.39		
Age	-.07	0.03	-.11 **	-2.78		
Frequency of Visits	.24	0.03	.31 ***	8.58		
Average Duration of Visits	.17	0.03	.18 ***	5.20		
Account Age	.01	0.00	.07 *	2.01		
Number of Friends	.00	0.00	.05	1.18		
Educational Level	-.03	0.05	-.02	-0.61		

*Note. *** indicates a significance at the 0.001 level, ** at the 0.01 level, and * at the 0.05 level. Males were assigned a value of 0, females a value of 1.*

As shown in Table 8 it was found that 51.4% of the variance of 'intention to disclose personal information' could be explained by the addition of the aforementioned predictors, adding 22.9% of the explained variance to the original research model. The number of Facebook-friends and the educational level both were not significant predictors for the respondents' intention to disclose personal information on OSNs, while the 'frequency of visits' is the second-strongest predictor (β = .31), followed by gender (β = .25). In addition, on a scale of 1 to 5, females scored higher (M = 2.86, SD = 0.73) on their intention to disclose personal than males (M = 2.29, SD = 0.91).

5 Discussion

As suggested by other researchers, this research included the influence of habits of personal information disclosure on OSNs, with success. The finding that the strongest predictor for the intention to disclose personal information were the respondents' habits, while this variable showed the lowest mean out of the 7 variables, is noteworthy. These results show that, although the respondents indicate that little of their disclosure of personal information is due to recurrent behavior that results from automatic processing of stimulus cues, the influence of these habits on their intention to disclose of personal information is substantial.

The second-strongest predictor for the intention to disclose personal information was the respondents' perceived control, with an exceptional high mean. This strong perception of control among the respondents, with no significant relation to their perceived privacy risks but a very significant and strong causal relationship with the intention to disclose personal information, is noteworthy.

The respondents' beliefs which reflected confidence that their personal information submitted to internet websites will be handled competently, reliably, and safely (i.e., *trust*) showed an above average mean. This indicates that the respondents trust that their personal information is save with the parties they have shared this information with. However, trust was not a significant predictor for the respondents' intention to disclose personal information. One could note that the decision to disclose personal information should not be viewed an indication of an individuals' trust, because even if there is no trust in the parties that can access the disclosed information, the expected benefits of disclosure could outweigh the costs. However, the high mean of the variable 'trust' compared to the low mean of the variable 'benefits' speaks against this argument.

The respondents' privacy valuation showed the highest mean of all the variables. This indicates that respondents' are convinced about the importance of their privacy. However, the correlation of the respondents' privacy valuation with their perceived privacy risks was insignificant and very weak, and although the predictive ability of the respondents' privacy valuation for their privacy concerns was significant, it was also weak.

It was proposed that an individuals' perceived privacy risks would negatively influence their intention to disclose personal information, which was not backed up by the findings. As mentioned in the theoretical framework, the literature discussing perceived privacy risks shows conflicting results. Similar results were found in other studies where, despite the risks, individuals continue to choose to disclose personal information. The low mean for the variable 'perceived privacy risks' could indicate that the decision to disclose personal information could be caused by unawareness of the possible risks.

The hypothesized influence of perceived control on perceived privacy risks was not significant with this sample. A possible explanation can be found when the questionnaire's items about perceived control are compared to those of the perceived privacy risks. There appears to be a mismatch between the questions; the items about the perceived control that Facebook's privacy and security settings offer the respondents do not offer protection to all the perceived privacy risks that are described in the items that cover this variable.

There appears to be a strong positive correlation between the perceived privacy risks and the benefits. An explanation for this correlation might lay in respondents' risk versus rewards calculus. Other authors already noted that internet users increasingly provided personal information on a voluntary basis for rewards or other benefits, as long as they overshadow the risks.

Although the results were checked for, and filtered from, social desirable answers, there were two important events that could have influenced the research's context. In September 2012 Facebook received a lot of negative attention in the Dutch press[3] after a party invite for a birthday party was unintentionally left open, and spiraled out of control, causing 'at least one million

[3] *for more information, see http://nl.wikipedia.org/wiki/Project_X_Haren*

euros' in damages to the town of Haren. In November 2012 a former student of the school where the research was conducted committed suicide, admittedly after being bullied his entire life. In addition to the (nationwide) attention to bullying, this tragic incident sparked a lot of discussions about harassment and (online) bullying. During this period, the school facilitated discussions in every class to discuss the dangers of OSNs. Both incidents were likely to have increased the students' awareness of the possible risks of sharing personal information online.

The fact that Facebook is such a popular network with a huge reach, and with unique properties and complexity, makes it interesting for research purposes. Although other OSNs share a lot of properties with Facebook, it appears that the sum is greater than its parts, which could result in complicating a comparisons with other OSNs.

5.1 Conclusions

This report offers a useful contribution to the current literature on information disclosure on OSNs, with a number of interesting findings. One of the strong points of this research is that the results in this report were based on a large number of questionnaires that were checked for the influence of social desirable responding by using a validated set of items, which increased the validity of the results.

This research's data confirms that habits apply well to the disclosure behavior on OSNs and it can be concluded that the proposed model's strongest predictor of an individual's intention to disclose personal information are one's habits. The perceived control, or the power to influence or direct personal information by selective disclosure and the right to select contacts without observation and intrusion, is the second strongest predicting variable. The final significant predictor for the intention to disclose personal information are the benefits that come from disclosing personal information.

Although current literature did not provided sufficient support for a causal relation between privacy valuation and trust and perceived control, the results from the regression analysis allow to conclude that there is a causal influence of trust on privacy valuation, and that there is a similar relation between perceived control and privacy valuation.

The results of the questionnaire also allow for some possibly distressing conclusions about the research sample. The respondents appear to be remarkably confident in the control they perceive to have over the personal information they disclose, which is also strong predictor for the similarly high valuation of their privacy. However, this perceived control has no significant relation with their perceived privacy risks, while the respondents indicate they do not perceive that much risks to their privacy in the first place. This does not seem to matter anyway, because the perceived privacy risks have no causal relation with the respondents' intention to share personal information.

In the meanwhile the strongest predictor of the respondents' intention to disclose personal information on OSNs are the result of automatic processing of stimulus cues, while the respondents themselves indicate that not much of their intention to disclose is habitual.

Finally, the scores for the respondents' trusting beliefs indicated that the respondents trust that their personal information will be handled competently, reliably, and safely by the parties they have shared this information with. The respondents' trusting beliefs appear to significantly lower their perceived privacy risks, but they have no a significant influence on their intention to disclose personal information.

6 Recommendations and Implications

This chapter will discuss the theoretical and practical implications of this research and offer suggestions for further research. The first and most advisable recommendation is to conduct *Structural Equation Modeling* (SEM) with the data that is obtained in this research. An overall measures of goodness-of-fit of the model should be computed.

Opportunities for further research are abundant. Considering the strong influence of habits, it is advised to further and more thoroughly investigate the influence of habits on disclosure in future research. Additionally, more research on habitual use across different demographic groups is suggested, as the substantially different use of OSNs is likely to result in different habits of disclosure on these platforms. This research only covered habits in disclosure, but as was shown in the last table of the results, the frequency and duration of the visits are strong predictors. Further research on the influence (and differences) of habitual use of OSNs on disclosure behavior are likely to provide interesting results.

The same applies to benefits; the strong influence of this variable is an interesting results that asks for further research. Because of the different core characteristics and uses of OSNs, as briefly discussed in the introduction of this report, more comprehensive research to the specific benefits of the different OSNs is highly advised.

The results that are obtained trough data-analysis, especially the correlation-figures, indicate that there are some unanticipated relations that should be further explored using SEM. For instance, there is a very strong positive correlation between habits and benefits. A possible explanation could be sought in the reasoning that beneficial results of information disclosure could result in a motivation to disclose more often, which in turn could resulting in habitual disclosure in the long run.

The results also show a strong positive correlation between the perceived privacy risks and benefits and a weaker but significant correlation between habits and the perceived privacy risks. SEM could provide more insight on these possible relations. The positive correlation between habits and perceived privacy risks is also interesting, because a negative correlation between the two variables would seem more logical; the more habitual the personal information disclosure is, the less privacy risks are perceived. However, the data suggests otherwise.

As mentioned before, one of the main defects of most privacy questionnaires and studies is that they do not separate out all of the different factors that could be considered privacy issues. Therefore, it is advised to investigate the factors that are considered as perceived privacy risks more thoroughly, and adjust the items in the research tool accordingly.

This research used a short version of the Marlowe Crowne's Social Desirability Scale to eliminate a portion of data that was very likely to contaminating the results. Researchers claim that a big proportion of the variance in participants' responses can be explained by SDR. Based on the findings in this research and the common knowledge among researchers about the influence of SDR on the validity of data gathered through self-reporting, it is surprising that the MCSDS-scales are hardly ever used in the social sciences. It is recommended that in future research that relies heavily on self-reporting, researchers look into the usefulness of the different MCSDS-scales that are available.

Current literature does not provide satisfying explanations for the influence of trust on privacy valuation and the similar relation between perceived control and privacy valuation. More research on these specific relations, and interaction between the two predictors, is highly suggested.

It appears that, although often criticized for their privacy policy and ambiguous preferences and settings, Facebook still gives the respondents an empowering sense of control over the personal information that has been disclosed by them. In addition, the respondents score exceptionally high on their privacy valuation. However, as noted in the conclusions, the bigger picture is that there appears to be no actual consequences to these seemingly good scores on the

perceived privacy risks or the intention to disclose personal information. These results can be seen as distressing for advocates of the importance of privacy.

This study can have some practical implications for schools; there appears to be a discrepancy between the possible risks of disclosing personal information that the school boards and teachers try to teach and warn adolescents about, and the actual consequences this knowledge has on their disclosure behavior. Further (qualitative) research could provide more in-debt insights on the presumptions that are based on data gathered from self-reporting, and test the findings of this study in real-life settings. This research should mainly focus on the role of the perceived privacy risks and its relations with other variables, because, as mentioned before, data shows that this variable appears to play a less crucial role than literature would suggest.

7 Acknowledgements

I would like to take this opportunity to thank some people that were important to me on during my master communication studies. First of all, I would like to thank my supervisors Ardion Beldad and Jan Gutteling for their knowledge, critical feedback, supportive words, and useful guidance during my master research. I experienced our meetings as pleasant, helpful, and refreshing.

Without my parents I would never even dared to start this whole journey. Thank you for your unconditional support, and the feeling that I could alway count on you, in every way possible. In addition, an even-more-special thanks to my mother for her on-sight coordination and distribution of the questionnaires, and communication with the teaching staff. You made the data-collection a breeze.

Annemiek, thank you for providing me with moral and nutritional support, validating my data-input, and listening to my boring rants about the dimensions of privacy (or trust, or habits, or control, or...). It means a lot! Jaap van der Zand, thank you for loudly announcing the first nine data-points of my questionnaire roughly four-hundred times. I appreciate your voice in this, all ±3,700 times.

Thank you school board, for enabling me to conduct this research with your students, and thanks to all the teachers for spending some of your valuable class time. A special thanks to Marcel Geesing, for believing in me and my research. I could, quite literally, not have done this without the support of every single one of you.

Finally, I would like to thank Thea van der Geest and Jan van Dijk for their inspiration, enthusiasm, experience, and knowledge they shared during the first part of my master course.

References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce* (pp. 1-8). ACM.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies* (pp. 36-58). Springer Berlin Heidelberg.

Acquisti, A., John, L., & Loewenstein, G. (2009). What is privacy worth. In *Workshop on Information Systems and Economics (WISE)*.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*(2), 107-123.

Augarde, A. J. (1981). *The Oxford Dictionary*. Oxford: Oxford UP.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869.

Beldad, A., De Jong, M., & Steehouder, M. (2011). A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet. *The Information Society, 27*(4), 220-232.

boyd, d. (2008). Facebook's Privacy Trainwreck. Convergence: The International Journal of Research into New Media Technologies, 14(1), 13-20.

boyd, d. (2009). Why youth ♥ social network sites: The role of networked publics in teenage social life. Retrieved March 2, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1518924

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology,58*(2), 157-165.

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, *7*(2), 117-141.

Cespedes, F. V., & Smith, H. J. (2012). Database marketing: new rules for policy and practice. *Sloan Management Review*. Retrieved July 9, 2013 from http://sloanreview.mit.edu/article/database-marketing-new-rules-for-policy-and-practice/

Cheung, C. M., & Lee, M. K. (2010). A theoretical model of intentional social action in online social networks. *Decision Support Systems*, *49*(1), 24-30.

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, R. (1999). Introduction to dataveillance and information privacy, and definitions of terms. *Roger Clarke's Dataveillance and Information Privacy Pages*.

Clarke, R. (2006). *What's 'Privacy'?* Retrieved June 2, 2013 from http://www.rogerclarke.com/DV/Privacy.html

Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of consulting psychology*, *24*(4), 349.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Das, T. K., & Teng, B. S. (1998). Between trust and control: developing confidence in partner cooperation in alliances. *Academy of Management review, 23*(3), 491-512.

Davis, K., & James, C. (2012). Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology*, 1-22.

De Souza, Z., & Dick, G. N. (2009). Disclosure of information by children in social networking—Not just a case of "you show me yours and I'll show you mine". *International Journal of Information Management*, *29*(4), 255-261.

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.

DeCew, J. W. (1997). In pursuit of privacy: Law, ethics, and the rise of technology. Cornell University Press.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422.

Donath, J., & boyd, d. (2004). Public displays of connection. *BT technology Journal*, *22*(4), 71-82.

Dwyer, C. (2007). Digital relationships in the 'MySpace' generation: Results from a qualitative study. In *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. In AMCIS (p. 339).

Ellison, N. B., Heino, R., & Gibbs, J. (2006). Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication*, *11*(2), 415-441.

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.

Gostin, L. O., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R., & Steinauer, D. D. (1993). Privacy and security of personal information in a new health care system. *JAMA: the journal of the American Medical Association*,*270*(20), 2487-2493.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153-160.

Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science, 9. Retrieved March 1, 2013 from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* 71-80, ACM.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence, 31*(1), 125-146.

Homans, G. C. (1958). Social behavior as exchange. *American journal of sociology*, 597-606.

Hui, K. L., Tan, B. C., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology (TOIT)*, *6*(4), 415-441.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. *Oxford handbook of Internet psychology*, 237-252.

Katz, J. E., & Rice, R. E. (2002). Social consequences of Internet use: Access, involvement, and interaction. MIT press.

Krasnova, H., Hildebrand, T., Günther, O., Kovrigin, S. and Nowobilska, A. (2008). Why Participate in an Online Social Networks: An empirical analysis, in W. Golden, T. Acton, K. Conboy, H. van der Heijden and V.K. Tuunainen, (eds.) Proceedings of 16th European Conference on Information Systems (Galway, Ireland; 2008), 2124–2135.

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. Retrieved March 3, 2013 from http://aisel.aisnet.org/amcis2009/343

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

Lankton, N. K., McKnight, D., & Thatcher, J. B. (2012). The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue Using a Social Networking Website. doi:d10.1109/TEM.2011.2179048

Lee, D. H., Im, S., & Taylor, C. R. (2008). Voluntary self-disclosure of information on the Internet: A multimethod study of the motivations and consequences of disclosing information on blogs. *Psychology & Marketing*,*25*(7), 692-710.

Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: the case of information systems continuance. *MIS Quarterly*, 705-737.

Lwin, M. O., Stanaland, A. J., & Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, *84*(2), 205-217.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior, 28*(4), 1471-1477.

Meztger, M. J. 2004. Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication 9*(4). Retrieved June 18, 2013 from http://jcmc.indiana.edu/vol9/issue4/metzger.html

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing*, 1-6.

Newell, P. B. (1995). Perspectives on privacy. *Journal of environmental psychology*, *15*(2), 87-104.

Nie, N. H. (2001). Sociability, Interpersonal Relations, and the Internet Reconciling Conflicting Findings. *American Behavioral Scientist*, *45*(3), 420-435.

Nie, N. H., & Erbring, L. (2000). Internet and society. *Stanford Institute for the Quantitative Study of Society*.

O'Brien, D. E. I. R. D. R. E., & Torres, A. M. (2012). Social Networking and Online Privacy: Facebook Users' Perceptions. *Irish Journal of Management*,*31*(2), 63-97.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243-262.

O'Murchu, I., Breslin, J. G., & Decker, S. (2004). Online social and business networking communities. In *Proceedings of ECAI 2004 Workshop on Application of Semantic Web Technologies to Web Communities*.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 27-41.

Qian, H., & Scott, C. R. (2007). Anonymity and Self-Disclosure on Weblogs. *Journal of Computer-Mediated Communication*, *12*(4), 1428-1451.

Quan-Haase, A., Wellman, B., Witte, J. C., & Hampton, K. N. (2002). Capitalizing on the net: Social contact, civic engagement, and sense of community. *The Internet in everyday life*, 291-324.

Reynolds, W. M. (1982). Development of reliable and valid short forms of the Marlowe-Crowne Social Desirability Scale. *Journal of clinical psychology*, *38*(1), 119-125.

Rezgui, A., Bouguettaya, A. R. A., & Eltoweissy, M. Y. (2003). Privacy on the Web: Facts, challenges, and solutions. *Security & Privacy, IEEE*, *1*(6), 40-49.

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13*(2), 183-192.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16* (3), 2-16.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management review*, *32*(2), 344-354.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21-32.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. *Interacting with Computers*, *22*(5), 428-438.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477-564.

Staksrud, E., & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication & Society*,*12*(3), 364-387.

Strater, K., & Richter, H. (2007). Examining privacy and disclosure in a social networking community. In *Proceedings of the 3rd symposium on Usable privacy and security,* 157-158, ACM.

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association*, *3*(1), 10-18.

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

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.

Van Deursen, A. J. A. M. & Van Dijk, J. A. G. M. (2012). Trendrapport internetgebruik 2012. Een Nederlands en Europees perspectief. Enschede: Universiteit Twente.

Van Dijk, J. (2012). *The Network Society*. SAGE Publications Limited.

Verplanken, B., & Orbell, S. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength1. *Journal of Applied Social Psychology*, *33*(6), 1313-1330.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220.

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication*, *17*(1), 101-115.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues, 59*(2), 431-453.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, *2*(4), 338-346.

Yan, Z. (2006). What influences children's and adolescents' understanding of the complexity of the Internet? *Developmental psychology*, *42*(3), 418.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389-418.

Appendix A: Questionnaire Items and Translated Item Texts

Table 1
Construct and translated item operationalization

Latent variable	Item	Item Text
Demographics (self-developed)	Dem1	What is your gender?
	Dem2	How old are you?
	Dem3	In what grade are you in?
	Dem4	Do you have a Facebook-account?
Intention to Disclose Personal Information (self-developed)	DPI1	I filled in my first name.
	DPI2	I filled in my last name.
	DPI3	I filled in my date of birth.
	DPI4	I filled in what town I live in.
	DPI5	I filled in where I work.
	DPI6	I filled in who my family members are.
	DPI7	I filled in if I have a relation.
	DPI8	I filled in my phone number.
	DPI9	I often use Facebook to keep my friends up-to-date on what I'm doing at that moment.
	DPI10	I often share my opinion on Facebook.
	DPI11	I often click 'Like' when I see something I like.
	DPI12	I often share on Facebook where I am at that moment.
	DPI13	I often share picture I'm in on Facebook.
	DPI14	I often react to pictures or messages of other Facebook-users.
	DPI15[1]	I often use the Facebook chat.
Habits (based on Verplanken & Orbell, 2003, p. 1329)	Hab1	How often do you visit Facebook?
	Hab2	How long are you approximately on Facebook per visit?
	Hab3	How long do you approximately own a Facebook-account?
	Hab4	How many Facebook-friends do you have approximately?
	Hab5	Sharing personal information is a habit to me.
	Hab6	I sometimes share personal information without thinking about it.
	Hab7	I sometimes share personal information because it is hard for me not to share it with others.
	Hab8	If I see something interesting, the first thing that comes into mind is to share it on Facebook.
Benefits (self-developed, based on Ellison *et al.*, 2006, p. 1151, and Krasnova *et al.*, 2010)	Ben1	Facebook is useful to exchange personal information with your friends.
	Ben2	Thanks to sharing personal information on Facebook, I get to know people better.
	Ben3	Facebook is useful for me to monitor what others share about themselves.
	Ben4	Sharing personal information on Facebook is fun.
	Ben5	On Facebook I have more courage in sharing personal information compared to other situations.
	Ben6	By sharing personal information on Facebook, I get more popular with my Facebook-friends.
	Ben7	I share personal information via Facebook because it's better than the alternatives.

Table 1
Construct and translated item operationalization

Latent variable	Item	Item Text
	Ben8	By sharing personal information on Facebook, I can make a good impression on my Facebook-friends.
Perceived Privacy Risks (self-developed, based on Dinev & Hart, 2004)	PPR1	Facebook as a company is a danger for the safety of my personal information.
	PPR2	I'm afraid that Facebook sells my personal information to others.
	PPR3	I'm afraid that Facebook secretly uses my personal information for purposes I don't agree with.
	PPR4	Friends-of-friends or companies on Facebook are a danger to my personal information.
	PPR5[1]	Hackers are a danger for my personal information on Facebook.
	PPR6	I'm afraid my Facebook-friends get a wrong impression of me because of the personal information I've shared on Facebook.
	PPR7	My Facebook-friends are a danger to the safety of my personal information.
	PPR8	I'm afraid my personal information can be used by my Facebook-friends to bully me with.
	PPR9[2]	I don't care about the risks of sharing personal information.
	PPR10	I'm afraid that I unintentionally share personal information because I made a mistake.
	PPR11	There are dangers to sharing personal information that I'm not aware of.
Privacy Valuation (self-developed)	PrV1	I think it's important that I keep control over my personal information.
	PrV2	I think that my personal information should be handled with care and respect.
	PrV3	I think it is important that I decide who can see and use my personal information.
	PrV4	I think that Facebook should do they best they can to protect my personal information.
Trust (self-developed, based on Krasnova *et al.*, 2010)	Tru1	I trust that Facebook has the expertise to handle my personal information.
	Tru2	Facebook has good intention for my personal information.
	Tru3	I trust that my Facebook-friends have the expertise to not jeopardize my personal information
	Tru4	I trust that my Facebook-friends don't do anything with my personal information I would not approve of.
	Tru5	I trust that my Facebook-friends keep my preferences and desires about my personal information in mind.
	Tru6	I trust that Facebook protects my personal information against companies and advertisers that want to abuse my information.
	Tru7	I trust that Facebook checks if everybody is playing by the rules.
Perceived Control (self-developed, based on Krasnova *et al.*, 2010)	PeC1[1]	I keep control over the things I shared on Facebook.
	PeC2	With the privacy-settings I determine who can see my personal information.
	PeC3	With the security-settings I can protect my personal information.
	PeC4	I have enough knowledge about Facebook to choose the settings that I think are most fitting.

Table 1
Construct and translated item operationalization

Latent variable	Item	Item Text
	PeC5[1]	I have sufficient expertise to not make any mistakes when I share personal information.
Social Desirability (Reynolds, 1982, based on Crowne & Marlowe, 1960)	SoD1	It's sometimes hard for me to go on with my work if I'm not encouraged.
	SoD2	I sometimes feel resentful when I don't get my way.
	SoD3[2]	No matter who I'm talking to, I'm always a good listener.
	SoD4	There have been occasions when I took advantage of someone.
	SoD5[2]	I'm always willing to admit when I made a mistake.
	SoD6	I sometimes try to get even rather than forgive and forget.
	SoD7[2]	I'm always courteous, even to people who are disagreeable.
	SoD8[2]	I have never been irked when people expressed ideas very different from my own.
	SoD9	There have been times when I was quite jealous of the good fortune of others.
	SoD10	I'm sometimes irritated by people who ask favors of me.
	SoD11[2]	I have never deliberately said something that hurt someone's feelings.

Note. [1] indicates an item that was removed after the reliability analysis, [2] indicates a reversed item. All items were to be rated on a 5-point Likert-Scale, ranging from 1 - 'Strongly Agree' to 5 - 'Strongly Disagree', except for: Dem1-4, Hab1-4, DPI1-8 ('No', 'Yes, but the info is incorrect', or 'Yes, and the info is correct'), and SoD1-11 ('Not true' or 'True').

Appendix B: Dutch Version of the Questionnaire

In deze vragenlijst komt de term ‘persoonlijke informatie’ veel voor. Omdat het voor ons belangrijk is dat je goed begrijpt wat wij er mee bedoelen, kun je hier nog een keer nalezen wat we er mee bedoelen: persoonlijk informatie is ***alle* informatie die *iets* vertelt over jou** als persoon. Op Facebook kan dit echt van alles zijn! Makkelijke en duidelijke voorbeelden zijn je naam, je leeftijd, of je geslacht. Of een foto van jou, je hond, of je lievelingseten. Maar ook een ‘Vind ik leuk’, een reactie, of waar je bent op dat moment. Zelfs vrienden die je *tagged* of een link naar je lievelingsnummer op *Youtube* zijn voorbeelden van persoonlijke informatie: het zegt of omschrijft allemaal iets over jou!

	Man	Vrouw
Wat is je geslacht?	o	o
Hoe oud ben je?		jaar
In welke klas zit je?		

	Nee, nooit gehad	Nee, niet meer	Ja
Heb je een Facebook-profiel?	o	o	o

Heb je bij deze vraag als antwoord ‘Nee’ gegeven? Dan ben je nu klaar!

	Meer dan tien keer per dag	Vijf tot tien keer per dag	Een tot vijf keer per dag	Paar keer in de week	Een keer per week of minder
Hoe vaak bezoek je Facebook?	o	o	o	o	o

	Minder dan een min.	Een tot vijf min.	Vijf tot vijftien min.	Vijftien min. tot een halfuur	Langer dan een halfuur
Hoe lang zit je ongeveer per keer op Facebook?	o	o	o	o	o
Hoe lang heb je ongeveer een Facebook-profiel?			jaar en		maand(en)
Hoeveel Facebook-vrienden heb je ongeveer?					

	Nee	Ja, maar de info klopt niet	Ja, en de info klopt
Ik heb mijn voornaam ingevuld.	o	o	o
Ik heb mijn achternaam ingevuld.	o	o	o
Ik heb mijn geboortedatum ingevuld.	o	o	o
Ik heb mijn woonplaats ingevuld.	o	o	o
Ik heb ingevuld waar ik werk.	o	o	o
Ik heb ingevuld wie mijn familieleden zijn.	o	o	o
Ik heb ingevuld of ik een relatie hebt.	o	o	o
Ik heb mijn telefoonnummer ingevuld.	o	o	o

	Zeer oneens	Redelijk oneens	Neu-traal	Redelijk eens	Zeer eens
Ik gebruik Facebook vaak om mijn vrienden op de hoogte te houden over wat ik op dat moment doe.	o	o	o	o	o
Ik deel vaak mijn mening op Facebook.	o	o	o	o	o
Ik klik vaak op *‘Vind ik leuk’* als ik iets zie wat ik leuk vind.	o	o	o	o	o
Ik deel vaak op Facebook waar ik op dat moment ben.	o	o	o	o	o
Ik zet vaak foto’s op Facebook waar ik op sta.	o	o	o	o	o
Ik reageer vaak op foto’s en berichten van andere Facebook-gebruikers.	o	o	o	o	o
Ik gebruik vaak de Facebook-chat.	o	o	o	o	o
Ik hou controle over wat er gebeurd met de dingen die ik op Facebook zet.	o	o	o	o	o
Met de privacy-instellingen kan ik bepalen wie mijn persoonlijke informatie kan zien.	o	o	o	o	o
Met de veiligheids-instellingen kan ik mijn persoonlijk informatie beschermen.	o	o	o	o	o
Ik weet genoeg over Facebook om de instellingen te kiezen die mij het beste lijken.	o	o	o	o	o
Ik ben deskundig genoeg om geen fouten te maken bij het delen van persoonlijke informatie.	o	o	o	o	o
Ik vind het belangrijk dat ik de controle hou over mijn persoonlijke informatie.	o	o	o	o	o
Ik vind dat er voorzichtig en met respect met mijn persoonlijke informatie om moet worden gegaan.	o	o	o	o	o

	Zeer oneens	Redelijk oneens	Neu-traal	Redelijk eens	Zeer eens
Ik vind het belangrijk dat ik kan beslissen wie mijn persoonlijke informatie mag zien en gebruiken.	o	o	o	o	o
Ik vind dat Facebook zo goed mogelijk hun best moet doen om mijn persoonlijke informatie te beschermen.	o	o	o	o	o
Ik vertrouw erop dat Facebook deskundig genoeg is om goed met mijn persoonlijke informatie om te gaan.	o	o	o	o	o
Facebook heeft goede bedoelingen met met mijn persoonlijke informatie.	o	o	o	o	o
Ik vertrouw er op dat mijn Facebook-vrienden genoeg weten over de instellingen om mijn persoonlijke informatie niet in gevaar te brengen.	o	o	o	o	o
Ik vertrouw erop dat mijn Facebook-vrienden geen dingen doen met mijn persoonlijke informatie die ik niet goed zou vinden.	o	o	o	o	o
Ik vertrouw erop dat mijn Facebook-vrienden rekening houden met mijn voorkeuren en wensen over mijn persoonlijke informatie.	o	o	o	o	o
Ik vertrouw erop dat Facebook mijn persoonlijke informatie goed beschermt tegen bedrijven en adverteerders die het willen misbruiken.	o	o	o	o	o
Ik vertrouw erop dat Facebook controleert of iedereen de regels nakomt.	o	o	o	o	o
Het delen van persoonlijke informatie is een gewoonte voor mij.	o	o	o	o	o
Ik deel wel eens persoonlijke informatie zonder er bij na te denken.	o	o	o	o	o
Ik deel wel eens persoonlijke informatie omdat ik het moeilijk vind om het niet met anderen te delen.	o	o	o	o	o
Als ik iets zie wat ik interessant of leuk vind, komt het direct in mij op om dit op Facebook te delen.	o	o	o	o	o

	Niet waar	Waar
Soms is het moeilijk voor mij om verder te gaan met mijn werk als ik niet word aangemoedigd.	o	o
Ik voel me soms vijandig als ik mijn zin niet krijg.	o	o
Het maakt niet uit met wie ik praat, ik ben altijd een goede luisteraar.	o	o
Ik heb wel eens gebruik van iemand gemaakt om er zelf beter van te worden.	o	o
Ik ben altijd bereid om het toe te geven als ik een fout maak.	o	o
Ik probeer soms wraak te nemen, in plaats van te vergeven en vergeten.	o	o
Ik ben altijd beleefd, zelfs voor mensen waar ik het niet mee eens ben.	o	o
Ik heb mij nooit geërgerd aan mensen die ideeën hebben die heel anders dan mijn eigen ideeën.	o	o
Ik ben wel eens heel jaloers op het geluk van anderen.	o	o
Soms raak ik geïrriteerd door mensen die mij om een gunst vragen.	o	o
Ik heb nog nooit met opzet iets gezegd dat iemand anders zijn gevoelens pijn deed.	o	o

	Zeer oneens	Redelijk oneens	Neu-traal	Redelijk eens	Zeer eens
Facebook is als bedrijf een gevaar voor de veiligheid van mijn persoonlijke informatie.	o	o	o	o	o
Ik ben bang dat Facebook mijn persoonlijke informatie verkoopt aan andere bedrijven.	o	o	o	o	o
Ik ben bang dat Facebook stiekem mijn persoonlijke informatie gebruikt voor dingen die ik niet goed vind.	o	o	o	o	o
Vrienden-van-vrienden of bedrijven op Facebook zijn een gevaar voor mijn persoonlijke informatie.	o	o	o	o	o
Hackers zijn een gevaar voor mijn persoonlijke informatie op Facebook.	o	o	o	o	o
Ik ben bang dat mijn Facebook-vrienden een verkeerd beeld van mij krijgen door de persoonlijke informatie die ik heb gedeeld.	o	o	o	o	o
Mijn Facebook-vrienden zijn een gevaar voor de veiligheid van mijn persoonlijke informatie.	o	o	o	o	o
Ik ben bang dat mijn persoonlijke informatie gebruikt kan worden door mijn Facebook-vrienden om mij mee te pesten.	o	o	o	o	o
De risico's van het delen van persoonlijke informatie kunnen mij niets schelen.	o	o	o	o	o

	Zeer oneens	Redelijk oneens	Neu-traal	Redelijk eens	Zeer eens
Ik ben bang dat ik door een eigen fout persoonlijke informatie deel die ik niet had willen delen.	o	o	o	o	o
Er zijn gevaren bij het delen van persoonlijke informatie waar ik niets van weet.	o	o	o	o	o
Facebook is handig om persoonlijke informatie uit te wisselen met je vrienden.	o	o	o	o	o
Dankzij het delen van persoonlijke informatie leer ik mensen beter kennen.	o	o	o	o	o
Via Facebook kan ik goed in de gaten houden wat anderen over zichzelf delen.	o	o	o	o	o
Persoonlijke informatie op Facebook delen is leuk.	o	o	o	o	o
Op Facebook durf ik meer persoonlijke informatie te delen dan in andere situaties.	o	o	o	o	o
Door persoonlijke informatie te delen word ik populairder bij mijn Facebook-vrienden.	o	o	o	o	o
Ik deel persoonlijke informatie via Facebook omdat het beter is dan de andere mogelijkheden.	o	o	o	o	o
Op Facebook kan ik door het delen van persoonlijke informatie een goede indruk maken op mijn Facebook-vrienden.	o	o	o	o	o

Heel erg bedankt voor het invullen van deze vragenlijst! Kijk je nog even snel of je niets bent vergeten of per ongeluk foutjes hebt gemaakt? Als je klaar bent mag je de vragenlijst weer inleveren bij je leraar.

Met de resultaten gaan wij vertrouwelijk om. Dat is ook de reden dat je geen naam op hoeft te geven, je blijft gewoon anoniem.

Ruud Koehorst

Appendix C: Additional Statistical Output

Table 1
Variable composition, item mean, and standard deviation.

Variable	Item	Mean	SD
Intention To Disclose Personal Information	DPI9	2.72	1.23
	DPI10	2.17	1.08
	DPI11	3.61	1.32
	DPI12	1.86	1.01
	DPI13	2.51	1.26
	DPI14	2.78	1.17
Trust	Tru1	3.95	1.02
	Tru2	3.38	1.00
	Tru3	3.66	0.95
	Tru4	3.94	0.91
	Tru5	3.76	0.92
	Tru6	3.73	1.09
	Tru7	3.39	1.16
Perceived Privacy Risks	PPR1	2.62	1.00
	PPR2	2.27	1.09
	PPR3	2.29	1.10
	PPR4	2.50	1.10
	PPR6	2.11	1.05
	PPR7	2.00	1.01
	PPR8	1.93	1.04
Benefits	Ben1	3.25	1.15
	Ben2	3.04	1.13
	Ben3	3.38	1.03
	Ben4	2.84	1.07
	Ben5	2.02	1.00
	Ben6	1.93	1.02
	Ben7	2.01	0.99
	Ben8	2.11	1.07
Privacy Valuation	PrV1	4.33	0.98
	PrV2	4.41	0.88
	PrV3	4.30	0.94
	PrV4	4.30	0.96
Perceived Control	PeC2	4.20	1.09
	PeC3	4.16	1.07
	PeC4	4.03	1.08
Habits	Hab5	2.42	1.12
	Hab6	2.20	1.17
	Hab7	1.87	1.01
	Hab8	2.15	1.10

Note. The value of the variables' mean could range from 1 to 5.

Table 2
Comparison of correct versus false personal information disclosed on the respondent's Facebook-profile, based on the age group.

	Correct information provided		Falsified information provided		No information provided		Falsification score
Respondents' age	Mean	SD	Mean	SD	Mean	SD	
12 (n = 38)	3.03	1.55	0.97	1.24	4.00	1.53	32%
13 (n = 94)	3.43	1.38	0.51	0.72	4.04	1.18	15%
14 (n = 109)	4.08	1.29	0.22	0.53	3.69	1.27	5%
15 (n = 139)	4.45	1.41	0.15	0.48	3.35	1.30	3%
16 (n = 89)	4.75	1.62	0.13	0.61	3.10	1.45	3%
17 (n = 22)	5.18	1.18	0.18	0.50	2.64	1.09	3%
All (N = 491)	4.15	1.53	0.30	0.69	3.53	1.36	7%

Note. The scores range from 0 to 8. The Falsification-score *indicates how often the respondents falsified information, compared to how often they provided correct information.*

Table 3
Comparison of time spend per visit, Facebook-account age, and number of Facebook-friends, based on frequency of visit.

	Time spend per visit		Facebook-account age (in years)		Number of Facebook-friends	
Respondents' frequency of visits	Mean	SD	Mean	SD	Mean	SD
More than 10 times a day (n = 40)	2.58	1.04	2.13	1.01	269	111.02
Five to ten times a day (n = 53)	2.64	0.86	2.04	0.77	293	140.67
Once to five times a day (n = 177)	2.64	0.83	1.75	1.07	197	138.87
A few times a week (n = 130)	2.70	0.85	1.50	1.01	168	142.69
Once a week, or less (n = 86)	1.98	0.83	1.42	1.13	84	96.02

Note. The scores for 'Time spend per visit' scores ranged from 1 to 5 and was categorical, but close to linear. The values for 'Facebook-account age' ranged from 1 to 6.2. The number of 'Facebook-friends' ranged from 2 to 800.