16/6/2016

DETERMINANTS OF PRIVACY PROTECTION BEHAVIOR ON SOCIAL NETWORK SITES: THE ROLE OF PRIVACY BELIEFS, SOCIAL NORMS AND INTERNET SKILLS.

M.H. VAN DER KAMP

MASTER THESIS

Determinants of privacy protection behavior on social network sites: The role of privacy beliefs, social norms and internet skills.

M.H. VAN DER KAMP, MAARTEN

1st Supervisor

DR. A.J.A.M. VAN DEURSEN, ALEXANDER

2nd Supervisor

DR. T.M. VAN DER GEEST, THEA

UNIVERSITY OF TWENTE.

FACULTY OF BEHAVIORAL, MANAGEMENT AND SOCIAL SCIENCES
DEPARTMENT OF COMMUNICATION STUDIES
SPECIALIZATION: MEDIA AND COMMUNICATION

16-06-2016

PREFACE

I have always found privacy one of the most important aspects of freedom. The developments in the world are driving people to give up their privacy in order to feel a little safer in this land of confusion. It seems that people are also willingly giving up their privacy for convenience. This bothers me a little because I feel that the lack of online privacy could create major problems for many people.

My worries for people's privacy have motivated me to start this study. During my quest I have spoken to many different people, and there are still persons who care about their privacy and are willing to learn how to protect their privacy online. But they did not always have the right skills and knowledge to protect their privacy, so I saw the opportunity and started a study about privacy behavior and internet skills. I chose to start with social network sites because I imagine when people do not even know how to protect their privacy on those platforms, how would they even know how to protect their data from online trackers.

I would like to say thanks to my supervisors Alexander van Deursen and Thea van der Geest for providing me with constructive feedback on my thesis during the process. I would also like to thank my family, friends and significant other for using their Facebook profiles in order to share my online survey.

Looking back on my progress during the whole master course I can honestly say that I have gave it my very best shot. I have learned a lot and I feel that I have gained the appropriate skills to do research, to reflect on myself, to reflect on my work and it has also changed the way I look at communication.

Wijchen, June, 2016

Maarten van der Kamp

ABSTRACT

This study examines the relationship of privacy beliefs, social norms and internet skills on online privacy protection behavior on social network sites using the theory of planned behavior as the underlying framework. An online survey was done among 282 Dutch persons and the data was analyzed with a path analysis. The results show that online privacy concern has the strongest positive relationship with online privacy protection behavior, then social skill, and then perceived vulnerability. Privacy disposition, perceived severity, subjective norm and self-efficacy have an indirect positive relation with online privacy protection behavior. The conclusion is that privacy beliefs have the greatest role in predicting online privacy protection behavior on social network sites. Social skills are necessary internet skills in order for people to protect their online privacy and social norms have a very small indirect role in determining online privacy protection behavior on social network sites. Future studies on privacy behavior should also include the effect of social skills since beliefs and attitudes are not sufficient in predicting online privacy protection behavior on SNS. There might be a possible gap in the perceived effectiveness of online privacy protection behavior and the actual effectiveness of online privacy protection behavior on SNS which deserves more attention in future studies. The implications of the study and future directions are discussed.

Keywords: online privacy protection behavior, social network sites, information privacy, internet skills, online privacy concern, privacy beliefs, theory of planned behavior.

Table of Contents

1. Introduction

Social network sites (SNS) are websites that connect people through internet-based technology. They enable people to connect and converse with each other, personally and in groups, synchronously as well as asynchronously. They enable people to play games with each other and share connections and updates such as stories, opinions, photo's, video's and events (boyd, 2010). Cybercriminals are using SNS as a platform for their scams (Rosdorff, 2016) and security software can only do so much. To feel safe, people engage in their own protective behaviors on SNS (Bartsch & Dienlin, 2016; Feng & Xie, 2014; Park, Campbell & Kwak, 2012). But there are also persons that actively engage in behaviors that could jeopardize their online safety even though they do not feel safe online (Baek, 2014; Hallinan & Friedewald & McCarthy, 2012; Rainie, Kiesler, Kang & Madden, 2013).

To define privacy, this study uses the definition of Westin (2003): *"privacy is the claim of an individual to determine what information about him or herself should be known to others" (p.3).* The absence of consumer control over personal information is central to most discussions of privacy and the process of maintaining your own privacy is strongly related with control over your own information (Taddei & Contena, 2013), especially on SNS.

This study aims to develop a greater understanding of the reasons why people engage in online privacy protection behavior on SNS and what skills are needed in order to perform this behavior. The main objective of this study is to investigate the role of privacy beliefs, social norms and internet skills in predicting online privacy protection behavior on SNS. A lack of belief in the effectiveness of protective measures might hinder people not to engage in protective behaviors (Hallinan et al., 2012). Additionally, the influence of social norms is also relevant for people to start protecting their privacy online (Feng & Xie, 2014; Taneja, Vitrana & Gengo, 2014; Zlatolas, Welzer, Hericko & Hölbl, 2015). Internet skills have been found to be an important determinant of online privacy protection behavior (Bartsch & Dienlin, 2016; Kurt, 2010; Park, 2011; Park et al., 2012). The privacy mechanisms of Facebook are too complicated for some of the users (Moll, Pieschl & Bromme, 2014). In addition, the levels of internet skills differ among the general population (Van Deursen & Van Dijk 2010), which might explain differences in privacy behavior on SNS. The research question is as following:

What is the role of privacy beliefs, social norms and internet skills on online privacy protection behavior on SNS?

This study uses the theory of planned behavior (Ajzen, 1991) as an underlying theoretical framework to investigate the determinants of online privacy protection behavior. The default privacy settings of SNS are "public" which means that all personal information can be seen by everyone. For people to start protecting their privacy such as blocking people, deleting old posts and adjusting the privacy settings to private, they need to perform intentional planned behavior.

This study contributes to the scientific literature by adding multiple internet skills in the model of online privacy protection behavior on SNS. When a certain type of skill has a greater relationship with online privacy protection behavior than the others, policy makers and educators could focus on that type of internet skill to improve people's privacy on SNS. When the most important determinants of online privacy protection behavior are known, it is less difficult to create effective policies and education programs to improve people's privacy on SNS.

First in chapter 2, the literature study will be reported to elaborate the different determinants of online privacy protection behavior. This results in a theoretical framework with hypotheses which form the foundation of the study. Subsequently in chapter 3, the research methods, instruments, procedures and the sample will be discussed. In chapter 4, the results of the research will be presented. Eventually in chapter 5, the conclusion and discussion with the main findings of the study will be presented together with the limitations of the study and directions for future studies.

2. THEORETICAL FRAMEWORK

2.1 THEORY OF PLANNED BEHAVIOR

The theory of planned behavior (TPB) (Ajzen, 1991) can be used to predict behavior and will be used as an underlying framework for this study. As presented in figure 1, intention and actual behavioral control are direct determinants of behavior. Intention is a representation of the person's readiness to perform a certain behavior. Actual behavioral control relates to a person's skills and resources to perform the behavior. Intention is determined by the combination of three different determinants; the attitude towards the behavior, the subjective norm and perceived behavioral control. The attitude towards the behavior relates to the beliefs of the person about performing the behavior. The subjective norm is the belief of the person about how others will view the behavior in question. The perceived behavioral control relates to the person's perception of their ability to perform the behavior. The perceived behavioral control also serves as a determinant for actual behavioral control and contributes to the behavior itself. The more favorable the attitude and subjective norm towards the behavior and the greater the perceived behavioral control, the higher the behavioral intention.

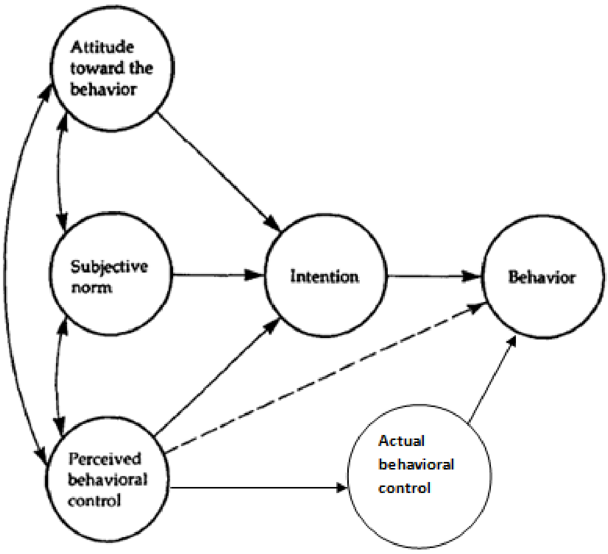

Attitude toward the behavior
Subjective norm
Intention
Behavior
Perceived behavioral control
Actual behavioral control

Figure 1. Theory of planned behavior (Ajzen, 1991)

In the current contribution, the theory will serve as a guideline to create the conceptual model to find the determinants of online privacy protection behavior. Because the actual (online privacy protection) behavior will be measured in this study, the actual behavioral control will be included in this study and the intention will be excluded. The determinants of intention (attitude towards the behavior, subjective norm and perceived behavioral control) will be directly tested on the behavior and the relationship between perceived behavioral control and actual behavioral control will be investigated.

2.2 ONLINE PRIVACY PROTECTION BEHAVIOR

In the TPB, the dependent variable is the behavior under investigation, in this case online privacy protection behavior on SNS. With online privacy protection behavior is meant the behavior an individual performs to protect his or her online information that in their perception should be kept private, from becoming available to others. Most SNS enable people to protect their privacy with different functions. Facebook has different privacy tool categories such as the option whether a profile will appear in search or whether a person can be tagged in photo's and posts by other people. Additionally, the privacy tool options give the possibility to share information with the public, friends of friends, friends or only yourself. Using these functions is a form of privacy protection behavior (Bartsch & Dienlin, 2016). Next to using these functions, people create their own sorts of behavior to protect their online privacy such as stop using the sites, giving false information (Park et al., 2012) and using steganography (Wolf, Willaert & Pierson, 2014). Steganography means using a slang or secret language so that it only becomes accessible to certain segments of your contacts. Also, not disclosing any information can be seen as a behavior to protect your online privacy on SNS. This study follows the conceptualization of online privacy protection behaviors on SNS as proposed by Feng and Xie (2014):

- Deleting people from your friend/network lists
- Removing your name from photo's where you are tagged in
- Deleting comments from others on your profiles
- Deleting or editing content you posted in the past
- Faking information such as name, age and location
- Blocking people
- Deactivating SNS accounts

Additionally, this study adds three more behaviors.

- Using the privacy-settings to set the visibility of your profile to friends-only (Bartsch & Dienlin, 2016)
- Encrypting messages so only friends understand your posts (Wolf et al., 2014)
- Refrain from posting information

When this study mentions online privacy protection behavior. It refers to the conceptualization of privacy protection behaviors above.

2.3 ATTITUDE TOWARDS THE BEHAVIOR

According to the theory of planned behavior, the attitude towards the behavior has impact on performing the actual behavior. Since this study aims to find out what role privacy beliefs have on online privacy protection behavior, the attitude towards privacy is added to the group attitude towards the behavior. The attitude towards the behavior is related to privacy beliefs since the behavior under investigation online privacy protection behavior is likely to be determined by beliefs about privacy. This study focuses on four different constructs related to the attitude towards the behavior; online privacy concern, privacy disposition, perceived vulnerability and perceived severity. In this study, these four constructs are categorized as privacy beliefs.

2.3.1 ONLINE PRIVACY CONCERN

Online privacy concern is defined as a person's overall perception of privacy risks and uncertainties that comes with disclosure of personal information on the Internet (Li, 2014^{a}).

It measures someone's overall perception and attitude of privacy risks in the online environment. These concerns can range from becoming a potential victim of cyber bullying to becoming a victim of data collection for marketing purposes. In this study, online privacy concern is a little bit different and defined as a person's overall perception of privacy risks and uncertainties that comes with disclosure of personal information on social network sites.

Online privacy concern is not specifically an attitude towards the behavior itself, but an attitude towards privacy uncertainties on SNS. The relationship between online privacy concern and online privacy protection behavior is found to be one of the strongest (Child & Starcher, 2016; Feng & Xie, 2014; Litt, 2013; Mohamed & Ahmad, 2012; Utz & Kramer, 2009), therefore it is included in the model. It is categorized here as attitude towards the behavior since it is a type of attitude, but the variable is placed in the model as a mediator between attitude towards the behavior, subjective norm and online privacy protection behavior (see figure 2).

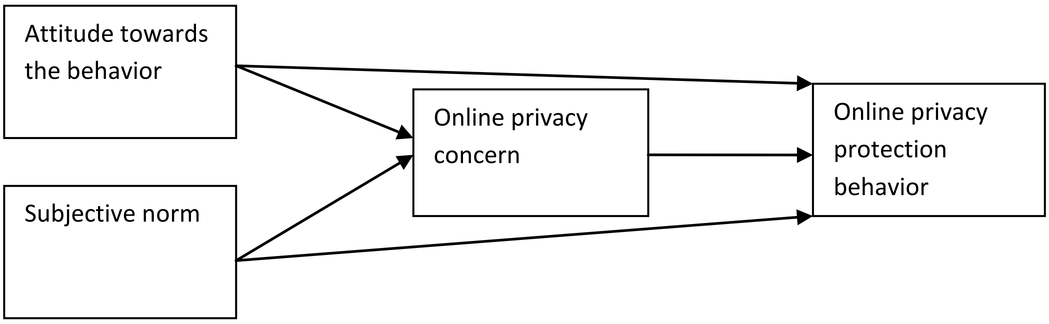

Attitude towards the behavior
Subjective norm
Online privacy concern
Online privacy protection behavior

Figure 2. Placement of online privacy concern in the conceptual model

Online privacy concern has a positive relation with on online privacy protection behavior (Feng & Xie, 2014; Mohamed & Ahmad, 2012) and SNS privacy tool use (Litt, 2013; Utz & Kramer, 2009). Additionally, online privacy concern has a negative relation with disclosure of personal information on social network sites (Zhou & Li, 2014). Feng and Xie (2014) defined online privacy concern as the concern about information being collected by marketers. Other studies (Litt, 2013; Mohamed & Ahmad, 2012; Utz & Kramer, 2009) defined online privacy concern as the worries and concerns people have about the accessibility and control of their personal information, which is more encompassing than concerns about data collection by marketers. Even though online privacy concern and online privacy protection behavior were defined differently in these studies, they all yield the result that online privacy concern has a positive relation with online privacy protection behavior. The hypothesis is:

H1: *Online privacy concern has a positive relation with online privacy protection behavior.*

2.3.2 PRIVACY DISPOSITION

Privacy disposition refers to an individual's fundamental beliefs about privacy (Li, 2014^{a}). It is defined as a person's general attitude about privacy values and psychological need for privacy across all contexts (Li, 2014[a]). It is often addressed as a characteristic or personality trait and mostly positioned as a determinant to other privacy beliefs such as online privacy concern (Li, 2014[a]; Li, 2014[b]).

Privacy disposition is not specifically an attitude towards the behavior itself, but an attitude towards privacy in general. This study suggests that the attitude towards using online privacy protection behavior is related to the attitude towards privacy in general since attitude towards using online privacy protection behavior is likely to be determined by beliefs and concerns about privacy. Therefore, privacy disposition is positioned in the category attitude towards the behavior.

To our knowledge, the direct relationship between privacy disposition and online privacy protection behavior has not been studied. However, a negative relationship was found between privacy disposition and intention to disclose personal information on a website (Li, 2014[a]). Persons who value their privacy highly are less likely to give their information which can be seen as type of online privacy protection behavior. This could also be applied on SNS. Therefore it is hypothesized that privacy disposition has a positive relationship with online privacy protection behavior.

H2a: *Privacy disposition has a positive relation with online privacy protection behavior.*

Privacy disposition is often positioned as a determinant to online privacy concern (Li, 2014[a]; Li, 2014[b]). In turn online privacy concern has a positive relation with online privacy protection behavior (Child & Starcher, 2016; Feng & Xie, 2014; Litt, 2013; Mohamed & Ahmad, 2012; Utz & Kramer, 2009). For this reason this study also includes the relationship between privacy disposition and online privacy concern.

Privacy disposition has a positive relationship with online privacy concern (Li, 2014[a]; Li, 2014[b]; Yao, Rice & Wallis, 2007). People have different beliefs about privacy rights and individuals that hold strong views about privacy rights will be more concerned about their online privacy than people that do not uphold such strong views (Yao et al., 2007). Conclusively, when a person values their privacy higher, this person is more likely to have higher online privacy concerns. The hypothesis is:

H2b: *Privacy disposition has a positive relation with online privacy concern.*

2.3.3 PERCEIVED VULNERABILITY

Perceived vulnerability is the belief whether an online threat (such as loss of privacy or harassment) will occur to the person (Dinev & Hart, 2004; Mohamed & Ahmad, 2012). It is defined as the perceived possible negative outcomes resulting from disclosing personal information on SNS (Dinev & Hart, 2004) and originates from the protection motivation theory (Rogers, 1975). It is studied across different contexts (e-commerce and SNS) and the perceived negative outcomes can range between credit card or ID fraud or feeling embarrassed due to a regretful SNS post.

Perceived vulnerability can be seen as an attitude towards disclosing information on SNS. Disclosing information can be seen as an opposite form of online privacy protection behavior. The more a person perceives disclosing information as a risky act, the more likely this person will generate a negative attitude towards disclosing information and a more positive attitude towards online privacy protection behavior.

People who expect a negative outcome as a result of information disclosure, are more likely to have online privacy concerns (Dinev & Hart, 2004; Mohamed & Ahmad, 2012), are less likely to disclose information and are more likely to use protective behaviors (Mohamed & Ahmad, 2012; Yuon, 2009). At the other hand, people who expect a positive outcome (e.g. a friendship or a job offer) as a result of information disclosure perceive less privacy invasion (Dinev & Hart, 2004) and thus are less likely to implement online privacy protection behavior. Those who stronger believe that a threat will occur to them are more likely to use online privacy protection behavior. The hypothesis is:

H3a: *Perceived vulnerability has a positive relation with online privacy protection behavior.*

Dinev and Hart (2004) investigated perceived vulnerability in relation to online privacy concerns. They separated the concerns in two groups, concerns about information being found and concerns about information being abused. Perceived vulnerability was found to have a positive relationship with both variables. Perceived vulnerability has a positive relation with online privacy concern in both e-commerce (Yuon, 2009) as in a social network setting (Mohamed & Ahmad, 2012). 51% of adolescents responded to have been victims of online harassment (Lwin, Li, & Ang, 2012). Therefore, it is important to include harassment in the perceived negative outcomes of this construct. People are also concerned about emotional discomfort, feeling guilty or regretful due to old posts, getting junk-mail (Yuon, 2009), being threatened, receiving sexual remarks (Lwin et al., 2012) or their information being made available to organizations and/or the government (Dinev & Hart, 2004). The hypothesis is:

H3b: *Perceived vulnerability has a positive relation with online privacy concern.*

2.3.4 Perceived severity

Perceived severity can be defined as a person's judgment of the severity of a consequence resulting from a threatening event or a problem due to disclosing personal information on SNS (Mohamed & Ahmad, 2012). Perceived severity also proceeds from the protection motivation theory (Rogers, 1975). Some persons might not take data collection or online harassment just as serious as others which might lead to different levels of online privacy concern and online privacy protection behavior. The perceived severity could partly explain why some people do not protect their SNS even though they have been victims of online harassment before (Lwin et al., 2012).

It seems that some people do perceive online problems serious but regard themselves unlikely to become victims (perceived vulnerability) even though 51% stated that they have been a victim of online harassment before (Lwin et al., 2012). Note that this might be because of optimistic bias; people tend to judge themselves as significantly less vulnerable to online risks than they judge others (Cho, Lee & Chun, 2010).

Perceived severity can be seen as an attitude towards possible privacy threats resulting from disclosing information on SNS. The attitude towards the possible threats might be important in determining whether the person should use protection behavior. Persons who receive hate mail but do not regard it as a serious problem might be less likely to implement online privacy protection behavior than persons who gets anxious by it.

Perceived severity (of harassment or online threats) is an important determinant for a person to start using protective behavior (Tsai, Jiang, LaRose, Rifon & Cotton, 2016). The greater the perceived severity, the higher the online privacy concern and the greater the chance a person will use behaviors in order to protect their privacy on SNS (Lwin et al., 2012; Mohamed & Ahmad, 2012). Perceived severity also negatively influences information disclosure, which can be seen as a protection strategy (Wang, Duong & Chen, 2016). When people experience possible threats and problems as a result of losing information privacy as more severe, they are more likely to have a higher online privacy concern and more likely to use online privacy protection behavior.

H4a: *Perceived severity has a positive relation with online privacy protection behavior.*

H4b: *Perceived severity has a positive relation with online privacy concern.*

2.4 Subjective norm

According to the theory of planned behavior, the subjective norm has impact on performing the actual behavior. Subjective norm can be defined as the perceived social pressure to engage or not engage in a certain behavior (Ajzen, 1991). Ergo, in this study it is defined as the perceived social pressure from friends, peers or family to engage in online privacy protection behavior on SNS. Users are more likely to use privacy controls when their friends and family are using them and when it is considered acceptable in their environment (Feng & Xie, 2014; Taneja et al., 2014; Zlatolas et al., 2015). People tend to fit in with others and tend to do what is expected of them, this is also strong on SNS since these are public environments if not effectively protected (Taneja et al., 2014).

There is a positive relationship between subjective norm (in favor of using privacy controls) and the intention to use privacy controls (Taneja et al., 2014). The more the perceived norms are in favor of using privacy settings, the higher the chance a person uses restrictive privacy settings (Utz & Kramer, 2009). However, the subjective norm goes both ways. When friends do not care about privacy, the person in question probably also has less care for its privacy. Additionally to a person's peers beliefs, social network contacts also influences a person's beliefs and behavior, people with Facebook friends that have private profiles are more likely to have private profiles themselves (Hofstra, Corten & Tubergen, 2016; Lewis, Kaufman &

Christakis, 2008). The subjective norm can emerge from different angles, as well in offline and online life. When friends and family expect an individual to share information freely on social network sites, the person will be less likely to use online privacy protection behavior and of course the other way around. In this study the subjective norm is in favor of using online privacy protection behavior. The hypotheses are:

H5a: *Subjective norm has a positive relation with online privacy protection behavior.*

H5b: *Subjective norm has a positive relation with online privacy concern.*

2.5 Perceived behavioral control

According to the theory of planned behavior, the perceived behavioral control has impact on performing the actual behavior and on the actual behavioral control. The perceived behavioral control relates to a person's perception of their ability to perform the behavior (Ajzen, 1991). This study distinguishes two different constructs related to perceived behavioral control; self-efficacy and response efficacy. The relationship between perceived behavioral control and actual behavioral control will be discussed in paragraph 2.6.2, after explaining the actual behavioral control.

2.5.1 Self-efficacy

Self-efficacy is a person's level of confidence and perceived ability to successfully perform a certain task (Dinev & Hart, 2006) and originates from the protection motivation theory (Rogers, 1975). It is a major determinant of people's choices of activities and how much effort they will put into it (Bandura, 1977). A higher self-efficacy leads to a higher chance of performing a certain behavior and a higher chance of being successful in it. Additionally, when people start performing the behavior in question, they will gain more confidence which in turn increases their self-efficacy (Bandura, 1991). Studies have shown that a scale for self-efficacy should be specially made for a certain domain rather than be measured with general measures (Bandura, 1989). In this study, self-efficacy is defined as a person's level of perceived general internet abilities and coping abilities of online problems (Yao et al., 2007). This definition of self-efficacy is chosen because the construct self-efficacy should be able to be investigated in relation with the different internet skills as well. Self-efficacy of online privacy protection behavior would be too specific to measure in relation with the different internet skills that will be used in this study.

In general, a higher self-efficacy leads to a higher chance of using internet (Eastin & LaRose, 2000). When a person believes he can perform a certain behavior, he is more motivated to persevere when problems arise (Bandura, 1989). A positive relationship was found between internet self-efficacy and online privacy protection behavior on SNS (Lwin et al., 2012). When persons are more confident in their online skills, they will be more likely to use them and successfully perform the task. The effect of self-efficacy was also found on technical protection strategies against identity theft in e-commerce (Lai, Li & Hsieh, 2012), using virus protection software (Lee, LaRose & Rifon, 2008) and using home wireless security (Woon et al., 2005). The hypothesis is:

H6: *Self-efficacy has a positive relation with online privacy protection behavior.*

2.5.2 Response efficacy

Response efficacy is the belief whether a certain coping response or protective behavior is effective in protecting against online threats and loss of privacy (Lwin et al., 2012; Mohamed & Ahmad, 2012). Response efficacy derives from the protection motivation theory (Rogers, 1975). It can be seen as perceived behavioral control because it is the perception of an individual whether the individual is in control of protecting themselves against online risks. According to protection motivation theory, the stronger the belief of the response efficacy, the more likely a person is to use this behavior (Rogers, 1975).

A positive relation was found between response efficacy and online privacy protection behavior among teenagers (Lwin et al., 2012), however this study focused on the response efficacy to protect yourself against online harassment and cyber bullying. However, the aim of this study is to incorporate a broader view of response efficacy, such as using protective behavior against losing your information privacy due to data collection and online threats. The results of this study could probably be generalized to adults as well since other studies have also found positive relations between response efficacy and privacy related behavior among adults. The response efficacy plays an important role in security behaviors in organizations (Herath & Rao, 2009), protecting against identity theft (Lai, Li & Hsieh, 2012), predicting strong passwords (Zhang & McDowell, 2009), backing up data (Crossler, 2010), intention to use anti-spyware software (Chenoweth, Minch & Gattiker, 2009), using anti-virus software (Lee et al., 2008) and using security for a home wireless network (Woon et al., 2005).

People normally take precautions in order to avoid risks if they believe they are effective, otherwise they might ignore the risk and refrain from taking action. The hypothesis is:

H7: *Response efficacy has a positive relation with online privacy protection behavior.*

2.6 Actual behavioral control

The actual behavioral control relates to a person's actual skills and resources to perform the behavior in question (Ajzen, 2002). In this study the actual behavioral control relates to the internet skills. As in the theory of planned behavior, actual behavioral control (internet skills) serves in the model as a mediator between perceived behavioral control and the behavior (see figure 3).

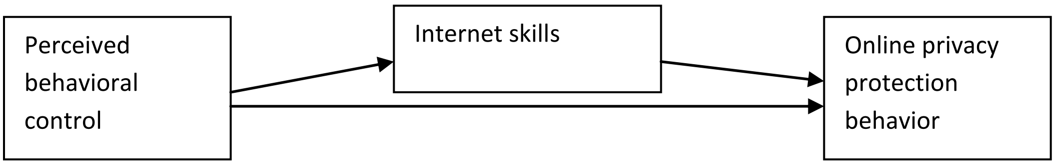

Perceived behavioral control
Internet skills
Online privacy protection behavior

Figure 3. Placement of internet skills (actual behavioral control) in the conceptual model

2.6.1 INTERNET SKILLS

In this study, internet skills are defined as the ability to use internet-connected devices (laptops, smartphones, tablets and personal computers) and internet applications to accomplish practical tasks (Dinev & Hart, 2006). Different forms of privacy-related skills are discussed in privacy literature. There is 'privacy knowledge' which relates to knowledge of data collection risk and awareness of regulatory protection and surveillance (Park, 2011; Park et al., 2012), and there is privacy literacy which refers to a person's ability to apply effective strategies for data protection (Bartsch & Dienlin, 2016). They both can be seen as a segment of the internet skills in the definition of Dinev and Hart (2006). But internet skills are more extensive than skills and knowledge about privacy, internet skills also encompass how to search, find the right information, validating sources, using operational buttons and knowing how and what to share online (Van Deursen, Helsper & Eynon, 2015).

When people are more skilled in using the internet, they have better understanding and are more aware of the risks of using the internet, subsequently increasing online privacy concern and online privacy protection behavior (Park, 2011). Furthermore, online privacy protection behavior is the highest for those with high levels of online concern and high levels of internet skills (Park et al., 2012). Kurt (2010) also explains that internet skills positively influence online privacy protection behavior. These studies are not focused on SNS but on the internet in general. It is expected that the relationships are similar when investigating SNS context. A study that focused on Facebook found a positive relation between the skills to use the privacy settings and the actual usage of the privacy settings (Bartsch and Dienlin, 2016), which is a part of online privacy protection behavior.

This study is going to use the internet skills constructs from Van Deursen et al. (2015). The scales of this study are the latest empirically tested and validated scales to measure different types of internet skills: operational, information navigation, social and creative skills.

Operational skill can be seen as 'button knowledge'. These skills are the basic skills of using the internet such as downloading/uploading files, using shortcut keys, adjusting privacy settings and watching videos (Van Deursen et al., 2015). Without operational skills it would be difficult to operate on the internet and people would not be able to use privacy settings and other online privacy protection behavior. Therefore this study hypothesizes that operational skills positively relates to online privacy protection behavior.

H8a: *Operational skill has a positive relation with online privacy protection behavior.*

Information navigation skill refers to people's skills to navigate while searching for information on the internet. It's about the ability to use the right keywords, verifying retrieved information and not getting lost on websites (Van Deursen et al., 2015). People with high information navigation skills are better in finding information than people with low information navigation skills. This study proposes that information navigation skill has a positive relation with online privacy protection behavior. People with high information navigation skills might probably have a higher perceived understanding of how easy it is to find personal information than people with low information navigation skills. Therefore they might be more likely to perform online privacy protection behavior. The hypothesis is:

H8b: *Information navigation skill has a positive relation with online privacy protection behavior.*

Social skill refers to the ability to know what information (not) to share, applying appropriate behavior in comments, knowing with whom to share information with and knowing how to contact or remove friends online (Van Deursen et al., 2015). When persons are more aware of the appropriateness and audiences of their online content, they might also be more aware of the privacy issues around social network sites. Having these skills probably increases the chance to perform online privacy protection behavior. The hypothesis is:

H8c: *Social skill has a positive relation with online privacy protection behavior.*

Creative skills are about knowing how to create and edit content such as pictures, video's and websites and publishing them in the online environment (Van Deursen et al., 2015). People who share content a lot are probably more familiar with the settings with whom they share their content with. They might also have experienced more persons reacting on their content which gives them more insight in how their privacy might be invaded. Hence, it is hypothesized that when persons has high creative skills, they are more likely to use online privacy protection behavior. However, when people share content, they might want to share it with the world which might lead to a decrease in their online privacy protection behavior. Even though when persons are active in sharing content, they might still want to protect their personal information and these skills might be helping in protecting their privacy. The hypothesis is:

H8d: *Creative skill has a positive relation with online privacy protection behavior.*

2.6.2 Effect of perceived behavioral control on actual behavioral control

In the theory of planned behavior, the actual behavioral control is influenced by the perceived behavioral control. In this study, these relationships will be investigated by looking at the relation of self-efficacy and response efficacy with internet skills.

Self-efficacy increases internet use (Eastin & LaRose, 2000) and in turn internet skills (Broos & Roe, 2006). A person with a high self-efficacy is more likely to perform a certain behavior and learn while performing it (Bandura, 1991). People tend to overestimate themselves; therefore self-efficacy is often used as a measure for perceived skills. It does not reflect actual skills but it serves as a determinant for internet skills (Helsper & Eynon, 2013). According to different studies, self-efficacy contributes positively to internet skills (Hatlevik, Guomundsdottir & Loi, 2015; Zhong, 2011) and is an important determinant for developing internet skills (Hatlevik, Ottestad & Trondsen, 2014). Therefore, this study proposes that self-efficacy has a positive relation with internet skills. Because this study divided internet skills in four different skills, the effect of self-efficacy on each skill will be investigated. The hypotheses are:

H9a: *Self-efficacy has a positive relation with operational skill.*

H9b: *Self-efficacy has a positive relation with information navigation skill.*

H9c: *Self-efficacy has a positive relation with social skill.*

H9d: *Self-efficacy has a positive relation with creative skill.*

When people believe that online privacy protection behavior will be effective, there might be a higher chance that the behavior will be performed. And performing the actual behavior might increase internet skills, similar as the effect between self-efficacy and internet skills. To our knowledge, the relationship between response efficacy and internet skills as characterized in this study has not yet been tested. Following the theory of planned behavior, this study would like to include this relationship and proposes that response efficacy has a positive relation with internet skills. Because this study divided internet skills in four different skills, the effect of self-efficacy on each skill will be investigated. The hypotheses are:

H10a: *Response efficacy has a positive relation with operational skill.*

H10b: *Response efficacy has a positive relation with information navigation skill.*

H10c: *Response efficacy has a positive relation with social skill.*

H10d: *Response efficacy has a positive relation with creative skill.*

2.7 CONCEPTUAL MODEL

The determinants are grouped according to the theory of planned behavior. Figure 4 shows the conceptual model with the hypotheses. The privacy beliefs; privacy disposition, perceived vulnerability and perceived severity are grouped in the attitude towards the behavior. They are positioned as direct determinants of online privacy concern and online privacy protection behavior. Online privacy concern is also a privacy belief but positioned as mediating variable between the other three privacy beliefs, subjective norm and online privacy protection behavior. Social norms are going to be measured by the construct subjective norm. The subjective norm is positioned as a direct determinant of online privacy concern and online privacy protection behavior. Self-efficacy and response efficacy is grouped in the perceived behavioral control and are direct determinants of online privacy protection behavior and internet skills. The four internet skills; operational skill, information navigation skill, social skill and creative skill are grouped in the actual behavioral control and are positioned between the perceived behavioral control and online privacy protection behavior.

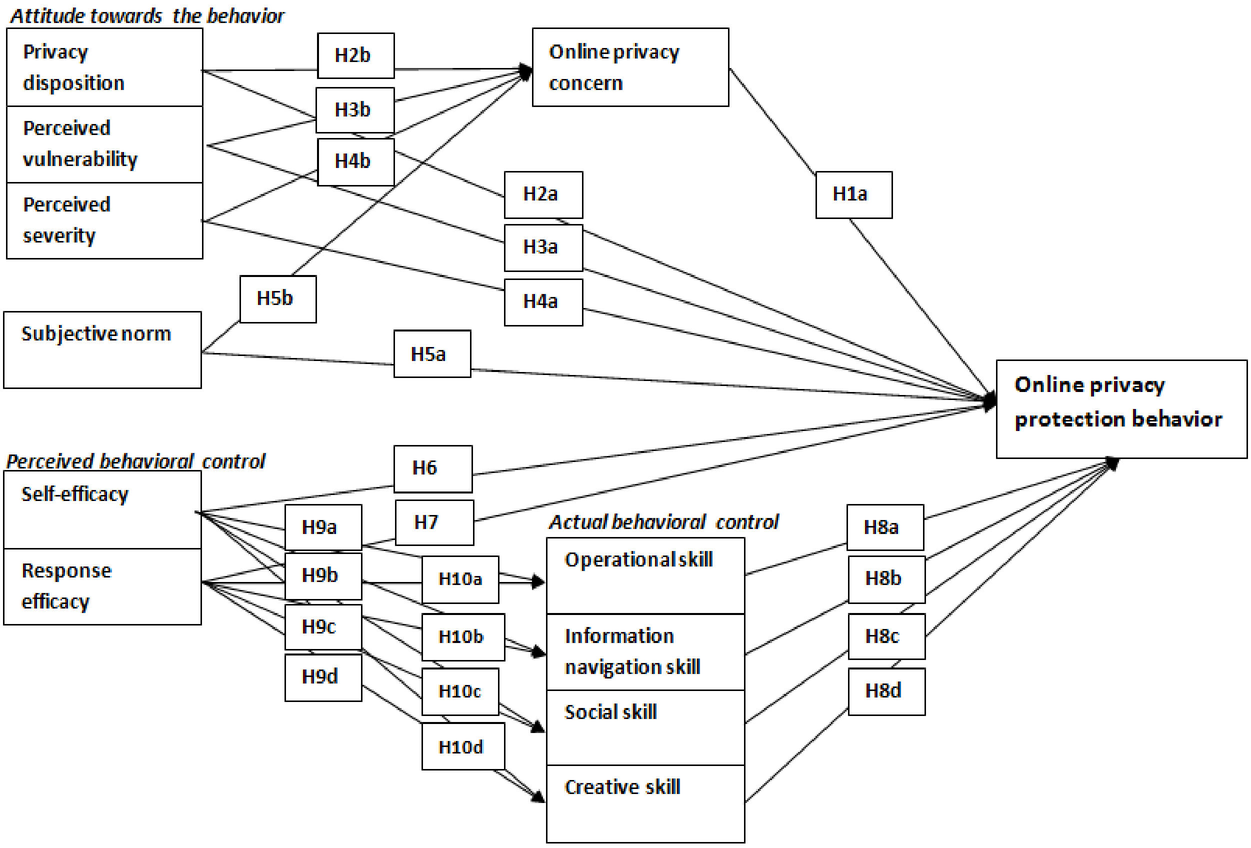


Figure 4. Conceptual model and proposed hypotheses.

3. METHOD

A total of 23 hypotheses are constructed to test the relationships between the different constructs. In order to measure the relationships between the constructs, this study used a quantitative research method; a cross-sectional correlational research with an online questionnaire. A path analysis was used to test the relationships between the constructs.

3.1 SAMPLE

This study draws upon a sample collected in the Netherlands during March 2016 by using an online questionnaire made in 'Qualtrics'. The link to the survey was distributed using snowball-sampling by e-mail and the social network sites LinkedIn and Facebook. Additionally, the link to the survey was distributed by mail in Wijchen. A total of 282 respondents completed the survey. Everyone above the age of 18 could participate.

3.2 INSTRUMENT

The survey was completely in Dutch because that is the native language of the participants. The survey started with an introduction with instructions, the reason of the study and with the message that participation is voluntary and anonymous. Afterwards, the participants had to fill in their demographic information, and then they had to fill in if they use social network sites. If they responded that they did not use social network sites, the survey would lead to the question why they do not use social network sites and afterwards the survey would close. The persons that did use social network sites went through the questionnaire with the constructs. All participants were thanked for their contribution and were presented with the contact information of the author for potential questions and remarks. To gauge reliability, a pre-test was done. The pre-test and the items of the constructs are elaborated in paragraph 3.4.

3.3 RESPONDENTS

A total of 374 persons started with the online questionnaire of which 26 respondents did not use any sort of social network sites and of which 11 persons where below the age of 18 and did not fit the target audience. After deleting the 55 participants that did not finish the entire questionnaire, a total of 282 useful respondent data remained. From the 26 respondents that did not use any social network sites, 12 reported that this was because of privacy related reasons. The model resulted in a Hoelter's *N* of 251 (at the .05 levels of significance) and 294 (at the .01 levels of significance), sufficient since sample size is adequate if Hoelter's *N* > 200.

Table 2 on the next page presents the age profile and table 3 on the next page presents the demographic profile. The average age is 40.14 (*SD* = 15.56). The participants are relatively young and highly educated. It is not a representative sample of the Dutch population.

Table 2. Age profile (*N* = 282)

Minimum	Maximum	Mean	Median	St. Dev
18	77	40.14	40.5	15.56

Table 3. Demographic profile (*N* = 282)

	N	%
Gender		
Male	144	51.1
Female	138	48.9
Age		
18-29	102	36.2
30-39	37	13.1
40-54	81	28.7
55-77	62	22
Education		
Low (e.g., middle school and high school)	20	7.1
Middle (MBO)	62	22
High (HBO)	117	41.5
University	83	29.4

3.4 Measures

3.4.1 Pre-test

A pre-test was conducted among 20 participants. The pre-test was done with 85 items with a 7-point likert scale (totally agree, agree, somewhat agree, neutral, somewhat disagree, disagree, totally disagree) and resulted in 50 remaining items in 12 reliable constructs. The pre-tested items and the remaining items with the corresponding alpha's can be found in Appendix A. The results of the pre-test and the construction of the constructs will be elaborated per construct.

Online privacy protection behavior (OPPB). The seven items of the scale of Feng and Xie (2014) were used to create the construct online privacy protection behavior. This scale was formerly a yes/no scale but was edited to make it fit in a likert agree/disagree scale. The scale exists of statements describing different privacy behaviors on social network sites. For example: *I sometimes delete people from my network or friends' list.* The author added three items with different protection behaviors which were not included in the scale of Feng and Xie (2014). A pre-test was done with 10 items of which six items remained; five items of Feng and Xie (2014) and one from the author. The scale resulted in an alpha of α = .76.

Online privacy concern (OPC). The scale for the construct OPC is from the study of Zlatolas, Welzer, Hericko and Hölbl (2015) which in turn constructed their scale with items from Dinev and Hart (2004) and Xu, Dinev, Smith and Hart (2008). Zlatolas et al. (2015) made the online privacy concern construct specifically applicable for social network sites. The items of the scale are statements about people's privacy concerns on social network sites. For example: *I am concerned that unauthorized people could access my personal information.* A total of five items were used in the pre-test of which four items remained with an alpha of α = .89.

Privacy disposition (PD). This scale was taken from the study of Li (2014). The scale is originally from Xu, Dinev, Smith and Hart (2011). Li (2014) edited the items for a better fit. The items asked the respondents to compare themselves with others regarding to their privacy beliefs. For example: *Compared to others, I see more importance in keeping personal information private.* The items were tested in the pre-test and resulted in an alpha of α = .96.

Perceived vulnerability (PV). To set-up the scale for perceived vulnerability, 7 items of the scale of Lwin et al., (2012) and 2 items of Dinev and Hart (2004) were used. The items of Dinev and Hart (2004) were edited to fit in the existing scale of Lwin et al., (2012). The study of Lwin et al. (2012) characterized perceived vulnerability as the perceived vulnerability to online threats and is focused on protection behavior against harassment. The items of Dinev and Hart (2004) focused on the perceived vulnerability of data being collected by the authorities and companies. The participants were asked whether they thought different online threats (*Receiving hate mail, being threatened, data being made available to the government*) would happen to them (*How likely do you think these issues will happen to you?).* They could answer with; very much not likely, not likely, somewhat likely, neutral, somewhat likely, likely, very much likely. After a pre-test with nine items, five items remained; three items of Lwin et al. (2012) and the two items of Dinev and Hart (2004). The scale resulted in an alpha of α = .8.

Perceived severity (PS). The items of the scale of perceived severity are almost the same as for perceived vulnerability. However, only the question is different. Participants were asked how serious they experience different online threats (*How serious are these issues to you?)* and they could answer with totally not serious, not serious, somewhat serious, neutral, somewhat serious, serious, totally serious. The pre-test was also done with nine items in which five remained with an alpha of α = .83. The same items remained as for the items of perceived vulnerability.

Subjective norm (SN). The items for this construct are from Zlatolas et al. (2015). The scale consists of three items. Participants were asked if they agree or disagree with statements describing whether they believe if their surroundings believe online privacy is important. For example: *Important friends believe that I need to take care about my privacy.* The pre-test resulted in an alpha of α = .82.

Self-efficacy (SE). For the construct of self-efficacy, ten items are used from the scale of Yao, Rice and Wallis (2007). This scale measures self-efficacy of general internet abilities and coping abilities of online problems. Participants were asked if they agree or disagree with statements describing whether they believe they can solve online problems easily, for example: *When I am in trouble online, I normally can think of a solution*. After the pre-test four items remained with an alpha of α = .87.

Response efficacy (RE). For this construct, 3 items of Mohamed and Ahmad (2012) and 2 of Lwin et al. (2012) were used. Additionally, the author added 4 items for translational convenience. Participants were asked whether they believe using protective measures is effective in protecting their online privacy. For example: *Using privacy settings on social network sites are beneficial to my privacy.* 9 items were used in the pre-test of which four remained. 3 of the author and 1 from Mohamed and Ahmad (2012). The pretest resulted in an alpha of α =.72.

Operational skill (OS). For this construct, the scale of Van Deursen, Helsper & Eynon (2015) was used. Participants had to agree or disagree with statements describing their operational skills such as knowing how to open new tabs (*I know how to open a new tab in my browser*), upload files and use shortcut keys. The pre-test was done with seven items of which four items remained. One of the items "I know how to change my privacy-settings" was moved to social skills after the pre-test due to a better fit. The pretest resulted in an alpha of α = .76.

Information navigation skill (INS). 7 items were used for this construct from the scale of Van Deursen et al. (2015). Participants were asked if they agree or disagree with statements describing their skills to navigate and find information on the internet. All items of this construct are reversed worded. Example: *Sometimes I find it hard to verify information I have retrieved.* After the pre-test four items remained with an alpha of α = .76.

Social skill (SS). For this construct the scale of Van Deursen et al. (2015) was used. Participants were asked if they agree or disagree with statements describing their online social skills such as knowing what information to share and with whom to share it with. For example: *I know how to change who I share content with (e.g. friends, friends of friends or public*. The scale originally had six items. Three items remained and one from operational skills "I know how to change my privacy-settings" was added. This resulted in a construct of 4 items with an alpha of α = .77.

Creative skill (CS). Six items were used in the pre-test from the scale of Van Deursen et al. (2015). Participants were asked if they agree or disagree with statements describing their creative internet skills such as creating content, developing websites and understanding licenses. For example: *I know which different types of licenses apply to online content*. Four items remained with an alpha of α = .85.

3.4.2 Final constructs

The definitive survey was done in a 5-point likert scale and can be found in Appendix A. A 5-point likert scale survey is generally more pleasant for the participant than a 7-point likert scale survey. Since the pre-tested constructs with the 7-point likert scale turned out to be reliable, the items were changed to a 5-point likert scale. All the questions were asked in an agree/disagree scale (agree, somewhat agree, neutral, somewhat disagree, disagree) except for perceived vulnerability and perceived severity. Table 4 (on the next page) provides the descriptive statistics for the items and scales with the corresponding alpha's used in this study.

Table 4. Descriptive statistics and Cronbach Alpha's for constructs and items

Items	Mean	St. Dev.	Author
Online Privacy Protection Behavior (OPPB) (α = .72)	**3.27**	**0.93**	Feng & Xie (2014)
1) I sometimes delete people from my network or friends' list.	3.95	1.33	
2) I sometimes remove my name from photos that I have been tagged on.	3.02	1.57	
3) I sometimes delete comments that others have made on my profiles or accounts.	2.66	1.52	
4) Sometimes, I delete or edit something that I posted in the past.	3.15	1.58	
5) I rarely block people. *(reverse-worded and recoded)*	2.52	1.43	
6) I often use the privacy-settings to set the visibility of my profile and online posts to friends only.	4.31	1.09	Author
Online Privacy Concern (OPC) (α = .85)	**4.06**	**0.90**	Zlatolas, Welzer, Hericko &Hölbl (2015)
1) It bothers me when I have to put much personal information on SNSs.	4.45	0.88	
2) I am concerned that SNSs are collecting too much personal information about me.	3.99	1.10	
3) I am concerned that unauthorized people could access my personal information.	3.76	1.19	
4) I am concerned that SNSs use my personal information for purposes that I am not being notified of.	4.03	1.12	
Privacy Disposition (PD) (α = .71)	**3.78**	**0.96**	Li (2014)
1) Compared to others, I am more concerned about the way other people or organizations handle my personal information.	3.56	1.15	
2) Compared to others, I see more importance in keeping personal information private.	3.99	1.02	
Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)	*dropped*		
Perceived Vulnerability (PV) (α = .78)	**2.63**	**0.75**	Lwin, Li & Ang (2012)
How likely do you think these issues will happen to you?			
1) Receiving hate emails.	1.99	0.93	
2) Being threatened online.	2.04	0.95	
3) Someone publishing my personal information online with bad intentions.	2.34	1.00	
4) My personal information being made available to the government.	3.35	1.15	Dinev & Hart (2004)
5) My personal information being made available to unknown companies or persons	3.45	1.12	
Perceived Severity (PS) (α = .84)	**3.81**	**0.96**	Lwin, Li & Ang (2012)
How serious are these issues to you?			
1) Receiving hate emails.	3.42	1.44	
2) Being threatened online.	3.58	1.44	
3) Someone publishing my personal information online with bad intentions.	4.10	1.15	
4) My personal information being made available to the government.	3.83	1.06	Dinev & Hart (2004)
5) My personal information being made available to unknown companies or persons	4.15	0.92	
Subjective Norm (SN) (α = .83)	**3.46**	**1.23**	Zlatolas, Welzer, Hericko &Hölbl (2015)
1) Important friends believe that I need to take care about my privacy.	3.45	1.32	
2) People who are important to me believe that I should be careful with exposing my information online.	3.48	1.33	
People who have influence on me believe that it is not very important to keep my personal information private. (reverse-worded)	*dropped*		
Self-efficacy (SE) (α = .79)	**3.91**	**0.91**	Yao, Rice, & Wallis (2007)
1) I get nervous when I have problems online. *(reverse-worded and recoded)*	3.48	1.33	
2) Normally I can find several solutions online.	4.09	1.06	
3) When I am in trouble online, I normally can think of a solution.	4.06	1.11	
4) I normally can handle whatever online problem that comes my way.	4.02	1.12	
Response Efficacy (RE) (α = .7)	**3.57**	**0.86**	Author
1) Using privacy settings on social networking sites makes me less likely to lose my information privacy.	3.80	1.05	
2) Using privacy settings on social network sites are beneficial to my privacy.	3.89	0.98	
3) Privacy settings on social network sites do not help protecting my privacy. *(reverse-worded and recoded)*	3.01	1.24	
I can protect my information privacy better if I use privacy protection measures in social networking sites.	*Dropped*		Mohamed & Ahmad (2012)
Operational Skill (OS) (α = .85)	**4.77**	**0.63**	Van Deursen, Helsper & Eynon (2015)
1) I know how to download/save a photo I found online.	4.79	0.72	
2) I know how to open a new tab in my browser.	4.80	0.72	

3) I know how to bookmark a website.	4.74	0.82	
4) I know how to upload files.	4.74	0.78	
Information Navigation Skill (INS) (α = .76) *(all reverse-worded)*	**2.72**	**1.05**	Van Deursen,
1) I find the way in which many websites are designed confusing.	2.69	1.23	Helsper &
2) All the different website layouts make working with the internet difficult for me.	2.32	1.29	Eynon (2015)
3) Sometimes I find it hard to verify information I have retrieved.	3.15	1.32	
I find it easy to decide what the best keywords are to use for online searches. (reverse-worded)	*dropped*		
Social Skill (SS) (α = .82)	**4.52**	**0.70**	Van Deursen,
1) I know which information I should and shouldn't share online.	4.53	0.85	Helsper &
2) I know when I should and shouldn't share information online.	4.54	0.88	Eynon (2015)
3) I know how to change who I share content with (e.g. friends, friends of friends or public).	4.59	0.82	
4) I know how to change my privacy-settings.	4.43	0.92	
Creative Skill (CS) (α = .72)	**3.19**	**1.11**	Van Deursen,
1) I know how to create something new from existing online images, music or video.	3.44	1.48	Helsper &
2) I know how to make basic changes to the content that others have produced.	3.32	1.48	Eynon (2015)
3) I don't know how to design a website. *(reverse-worded and recoded)*	2.81	1.66	
4) I know which different types of licenses apply to online content.	3.20	1.42	

Note. Five-point likert scale.

Online privacy protection behavior (OPPB). A 6-item scale was used to measure individual privacy protection behaviors on social network sites. The construct displayed sufficient internal consistency (α = .72).

Online privacy concern (OPC). Four items were used for the construct online privacy concern. The construct displayed good internal consistency (α = .85).

Privacy disposition (PD). Three items were used for this construct. The item "Compared to others, I am less concerned about potential threats to my personal privacy" was dropped due to a lack of internal consistency and two items remained with an internal consistency of α = .71.

Perceived vulnerability (PV). Five items were used to measure an individual's perceived vulnerability. The construct displayed sufficient internal consistency (α = .78). Instead of an agree/disagree scale, the question for perceived vulnerability was *How likely do you think these issues will happen to you?* And the answers were: very much not likely, not likely, neutral, likely, very much likely.

Perceived severity (PS). The items of the scale of perceived severity are almost the same as for perceived vulnerability. The construct displayed good internal consistency (α = .84). Instead of an agree/disagree scale, the question for perceived severity was *How serious are these issues to you?* And the answers were: totally not serious, not serious, neutral, serious, totally serious.

Subjective norm (SN). Three items were used for this construct. The item "People who have influence on me believe that it is not very important to keep my personal information private" was dropped due to a lack of internal consistency and two items remained with an internal consistency of α = .83.

Self-efficacy (SE). Four items were used for this construct. The construct displayed a sufficient internal consistency (α = .79).

Response efficacy (RE). Four items were used to measure a person's response efficacy. The item "I can protect my information privacy better if I use privacy protection measures in social networking sites" was dropped due to a lack of internal consistency and three items remained with an internal consistency of α = .7.

Operational skill (OS). Four items were used to measure an individual's operational skills. The construct displayed good internal consistency (α = .85).

Information navigation skill (INS). Four items were included for the construct for information navigation skills. Eventually three items remained after dropping the item "I find it easy to decide what the best keywords are to use for online searches" and three items remained with an alpha of α =.76. In this construct all items are reversed-worded.

Social skill (SS). Four items were used for the construct social skills. The construct shows good internal consistency (α =.82).

Creative skill (CS). A 4-item scale was used for the construct creative skills. The construct displayed sufficient internal consistency (α = .72).

3.5 DATA ANALYSIS

To test the hypotheses and the relationships as presented in the model, a total score was calculated from each construct and a correlation analysis was done. Next, the model was tested with a path analysis using AMOS 20.0. To obtain a comprehensive model fit, the χ2 statistic, the ratio of χ2 to its degree of freedom (χ2/df), the standardized root mean residual (SRMR), the Tucker-Lewis index (TLI) and the root mean square error of approximation (RMSEA) were included.

4. Results

This chapter presents the results of the research, the research question is: What is the role of privacy beliefs, social norms and internet skills on online privacy protection behavior on SNS? To obtain the results, a correlation analysis and a path analysis was done. The first research model did not fit; therefore the model was improved with new paths suggested by the program AMOS 20.0. After the improvement, the hypotheses were tested in the new research model.

4.1 Structural model

The results obtained from testing the validity of a causal structure of the conceptual model in figure 4 are as follows: χ2 (36) =125.833; χ2/df=3.495; TLI=.722; RMSEA=.094 (90% confidence interval [CI] = .077, .112). A significant chi-squared value indicates a lack of satisfactory model fit. For improvement, nine new paths were added between the following constructs: from privacy disposition to perceived vulnerability, privacy disposition to perceived severity, perceived severity to perceived vulnerability, perceived severity to subjective norm, self-efficacy to subjective norm, response efficacy to online privacy concern, operational skill to subjective norm, information navigation skills to perceived vulnerability and social skill to perceived vulnerability. Additionally, positive correlations were found between the different internet skills; operational skill and information navigation skill (*r* = .25), operational skill and social skill (*r* = .44), operational skill and creative skill (*r* = .30), information navigation skill and social skill (*r* = .27), information navigation skill and creative skill (*r* = .39) and social skill and creative skill (*r* = .41). These constructs are added as covariates in the new model. Furthermore, a significant negative correlation was found between privacy disposition and information navigation skill (*r* = -.18), this was not part of the first research model but due to the correlation, these two constructs were added as covariates in the new model. All correlations can be found in table 5 below.

Table 5. Pearson correlations

Construct	1	2	3	4	5	6	7	8	9	10	11	12
1. OPPB	1	.24**	.22**	.17**	.20**	.11	.07	.09	.18**	.07	.21**	.14*
2. OPC		1	.48**	.22**	.38**	.21**	-.11	-.24**	-.06	-.25**	-.16**	-.14*
3. PD			1	.17**	.29**	.11	.03	-.09	.07	-.18**	.04	.13*
4. PV				1	.20**	.03	-.07	-.05	.01	-.12	-.15*	.02
5. PS					1	.16**	-.09	-.08	.05	-.14*	-.04	-.06
6. SN						1	-.12*	.01	-.16**	-.18**	-.02	-.11
7. SE							1	.11	.45**	.42**	.44**	.55**
8. RE								1	.06	. 15*	.22**	.13*
9. OS									1	.25**	.44**	.30**
10. INS										1	.27**	.39**
11. SS											1	.41**
12. CS												1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

After improvement the basic assumptions for structural equation modeling were met. The changes resulted in a model with good fit and a non-significant chi-squared value: χ2 (27) =44.932; χ2/df=1.664; SRMR=.201; TLI=.926; RMSEA=.049 (90% confidence interval [CI] = .021, .073).

The analyses were done on the new adjusted model. The model explains 20% of the variance in online privacy protection behavior, 34% in online privacy concern, 20% in operational skill, 18% in information navigation skill, 21% in social skill, 30% in creative skill, 8% in perceived vulnerability, 9% in perceived severity and 6% in subjective norm.

4.2 PRIVACY BELIEFS

The standardized path coefficients indicate a significant direct positive relation between online privacy protection behavior and online privacy concern (β = .22, *p* <.001). The hypotheses, H1: Online privacy concern has a positive relation with online privacy protection behavior – is accepted. This means that online privacy concern has a direct role in predicting online privacy protection behavior.

Privacy disposition has an indirect positive relation with online privacy protection behavior (β = .10) due to the direct relationships with online privacy concern (β = .38, *p* <.001) and perceived severity (β = .29, *p* <.001). The relationship works through the path of online privacy concern to online privacy protection behavior, through the path of perceived severity to online privacy concern to online privacy protection behavior and through the path of perceived severity to perceived vulnerability to online privacy protection behavior. Therefore, H2a: Privacy disposition has a positive relation with online privacy protection behavior – is partially accepted and H2b: Privacy disposition has a positive relation with online privacy concern – is accepted. Additionally, an indirect positive relation was found between privacy disposition and perceived vulnerability via the path of perceived severity (β = .05). Also, an indirect positive relationship was found between privacy disposition and online privacy concern via the path of perceived severity (β = .06) which gives privacy disposition a total effect of β = .44 on online privacy concern. This means that privacy disposition has a direct role in predicting online privacy concern and predicting perceived severity. And an indirect role in predicting online privacy protection behavior and perceived vulnerability.

Direct positive relationships between perceived vulnerability and online privacy protection behavior (β = .13, *p* = .04) and between perceived vulnerability and online privacy concern (β = .10, *p* <.04) have been found. Hereby supporting both hypotheses. H3a: Perceived vulnerability has a positive relation with online privacy protection behavior – is accepted. H3b: Perceived vulnerability has a positive relation with online privacy concern – is accepted. Additionally, perceived vulnerability has an indirect positive relation with online privacy protection behavior via the path online privacy concern (β = .02). Hereby the effect of perceived vulnerability on online privacy protection behavior comes to a total of β = .15. The results show that perceived vulnerability plays a direct role in predicting online privacy protection behavior and online privacy concern.

Perceived severity has a direct positive relation with online privacy concern (β = .22, *p* <.001), and indirectly with online privacy protection behavior (β = .07) through the paths of online privacy concern (β = .05) and perceived vulnerability (β = .02). Thus, H4a: Perceived severity has a positive relation with online privacy protection behavior – is partially accepted. H4b: Perceived severity has a positive relation with online privacy concern – is accepted. Additionally, perceived severity has a direct positive relation with perceived vulnerability (β = .16, *p* = .009) which leads to an indirect positive effect of perceived severity on online privacy concern (β = .02). Furthermore, perceived severity also has an indirect positive relation with online privacy concern through the path of subjective norm (β = .02) which leads to a total effect of β = .26 between perceived severity and online privacy concern. Perceived severity plays a direct role in predicting online privacy concern and perceived vulnerability which indirectly determines online privacy protection behavior.

The role of privacy beliefs is prominent in determining online privacy protection behavior. All different privacy beliefs positively influence each other within the group. The privacy beliefs; privacy disposition, perceived vulnerability and perceived severity all have a direct positive role in determining online privacy concern which in turn is the greatest positive determinant of online privacy protection behavior. Perceived vulnerability also has a direct positive role in determining online privacy protection behavior.

4.3 SOCIAL NORMS

A direct positive relation has been found between subjective norm and online privacy concern (β = .13, *p* <.008), which leads to an indirect positive relationship with online privacy protection behavior (β = .03). A significant direct relation between subjective norm and online privacy protection behavior was not found. H5a: Subjective norm has a positive relation with online privacy protection behavior – is partially accepted. H5b: Subjective norm has a positive relation with online privacy concern – is accepted. Additionally, Perceived severity has a direct positive relation with subjective norm (β = .16, *p* = .006). This means that the perceived severity plays a role in determining the subjective norm or the other way around.

Social norms and privacy beliefs are linked with each other. Online privacy concern and perceived severity relates with the subjective norm. However, the role of social norms in determining online privacy protection behavior is an indirect one and very small.

4.4 PERCEIVED BEHAVIORAL CONTROL

Self-efficacy has an indirect positive relation with online privacy protection behavior via social skill (β = .08). A direct effect was not found. H6: Self-efficacy has a positive relation with online privacy protection behavior – is partially accepted. Self-efficacy partially determines a person's online privacy protection behavior. The effects of self-efficacy on the internet skills are elaborated in the next paragraph.

Response efficacy has a negative indirect relation with online privacy protection behavior (β = -.01). A direct negative relation was found between response efficacy and online privacy concern (β = -.19, *p* <.001). And a positive relation was found between response efficacy and social skill (β = .17, *p* =.001). The indirect relationship has been found through the path of social skill (β = .03) and online privacy concern (β = -.04). The effect between response efficacy and online privacy concern is slightly larger than the effect between response efficacy and social skill which leads to a minor negative indirect relationship. Thus rejecting the hypothesis. H7: Response efficacy has a positive relation with online privacy protection behavior – is rejected. Response efficacy has a very small indirect negative relationship with online privacy protection behavior and plays a small role in predicting online privacy protection behavior.

The perceived behavioral control does not have a major influence in determining online privacy protection behavior. The effects are small and indirect.

4.5 Internet skills

A positive direct effect was found between online privacy protection behavior and social skill (β = .19, *p* = .003). All other relations between online privacy protection behavior and the internet skills are not significant. H8a: Operational skill has a positive relation with online privacy protection behavior – is rejected. H8b: Information navigation skill has a positive relation with online privacy protection behavior – is rejected. H8c: Social skill has a positive relation with online privacy protection behavior – is accepted. H8d: Creative skill has a positive relation with online privacy protection behavior – is rejected. The results also show that social skill has a direct negative relation with perceived vulnerability (β = -.14, *p* = .02) which leads to a small indirect negative effect on online privacy protection behavior (β = -.02). The total effect between online privacy protection behavior and social skill is β = .17. This means that social skill leads to a lower level of perceived vulnerability and to a higher level of online privacy protection behavior. Furthermore, operational skill negatively relates with subjective norm (β = -.15, *p* = .021).

The internet skills altogether seem not to have a large role in determining online privacy protection behavior. But individually, social skill plays a major role in determining online privacy protection behavior. Social skill has the largest role in determining online privacy protection behavior after online privacy concern. A higher level of social skill also leads to a lower level of perceived vulnerability. Additionally, a higher level of operational skill leads to a lower level of social norm. Thus internet skills also influence privacy beliefs and social norms to a certain extent.

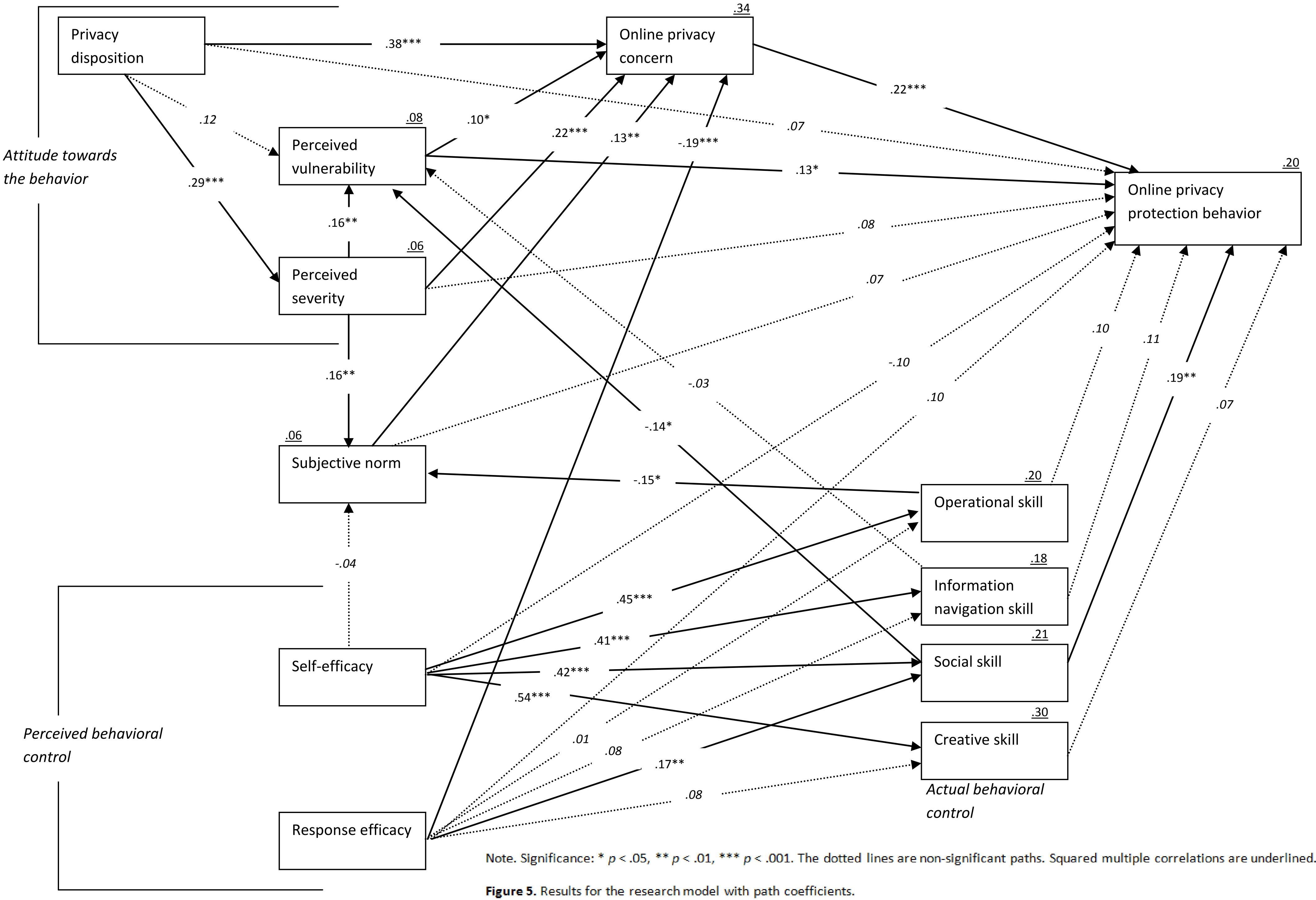
The results found positive relations between self-efficacy and operational skill (β = .45, *p* <.001), self-efficacy and information navigation skill (β = .41, *p* <.001), self-efficacy and social skill (β = .42, *p* <.001) and self-efficacy and creative skill (β = .54, *p* <.001). H9a: Self-efficacy has a positive relation with operational skill – is accepted. H9b: Self-efficacy has a positive relation with information navigation skill – is accepted. H9c: Self-efficacy has a positive relation with social skill – is accepted. H9d: Self-efficacy has a positive relation with creative skill – is accepted. This means that self-efficacy plays a large direct role in determining internet skills. A higher self-efficacy leads to higher skills.

A positive relation was found between response efficacy and social skill (β = .17, *p* =.001). The other relationships between response efficacy and internet skills are not significant. H10a: Response efficacy has a positive relation with operational skill – is rejected. H10b: Response efficacy has a positive relation with information navigation skill – is rejected. H10c: Response efficacy has a positive relation with social skill – is accepted. H10d: Response efficacy has a positive relation with creative skill – is rejected. This means that response efficacy plays a direct role in determining social skill.

The perceived behavioral control plays a large role in determining internet skills. Especially self-efficacy plays a major role in determining internet skills. The effect of response efficacy only applies to social skill.

4.6 PATH MODEL

Figure 5 on the next page provides the comprehensive path model with the coefficients and variances explained, the full arrows show the significant paths and the dotted lines are the non-significant paths.



Note. Significance: * *p* < .05, ** *p* < .01, *** *p* < .001. The dotted lines are non-significant paths. Squared multiple correlations are underlined.

Figure 5. Results for the research model with path coefficients.

4.7 HYPOTHESIS TESTING

Table 6 summarizes the validation of the hypotheses with the corresponding direct and indirect effect values and table 7 presents the effects and sigma's of the paths that have been added to the adjusted model. Based on the results, 12 out of 23 hypotheses are supported and 4 are partially supported.

Table 6. Significant direct, indirect and total effects on hypotheses

Link	Direct effect β	Indirect effect β	Total effect β	Validation
H1: OPC→ OPPB	.22	-	.22	Supported
H2a: PD→OPPB	-	.10	.10	Partially supported
H2b: PD→OPC	.38	.06	.44	Supported
H3a: PV→OPPB	.13	.02	.15	Supported
H3b: PV→OPC	.10	-	.10	Supported
H4a: PS→OPPB	-	.07	.07	Partially supported
H4b: PS→ OPC	.22	.04	.26	Supported
H5a: SN→OPPB	-	.03	.03	Partially supported
H5b: SN→OPC	.13	-	.13	Supported
H6: SE→OPPB	-	.08	.08	Partially supported
H7: RE→OPPB	-	-.01	-.01	Rejected
H8a: OS→OPPB	-	-	-	Rejected
H8b: INS→OPPB	-	-	-	Rejected
H8c: SS→OPPB	.19	-.02	.17	Supported
H8d: CS→OPPB	-	-	-	Rejected
H9a: SE→OS	.45	-	.45	Supported
H9b: SE→INS	.41,	-	.41	Supported
H9c: SE→SS	.42	-	.42	Supported
H9d: SE→CS	.54	-	.54	Supported
H10a: RE→OS.	-	-	-	Rejected
H10b: RE→INS	-	-	-	Rejected
H10c: RE→SS	.17	-	.17	Supported
H10d: RE→CS	-	-	-	Rejected

Table 7. Effects on the added paths and sigma

Link	Effect (β)	Sigma (p)
PD→PV	*.12*	*.051 (NS)*
PD→PS	.29	<.001
PS→PV	.16	.009
SS→PV	-.14	.02
OS→SN	-.15	.021
PS→SN	.16	.006
INS→PV	*-.03*	*.580 (NS)*
SE→SN	*-.04*	*.523 (NS)*
RE→OPC	-.19	<.001

5. Discussion and conclusions

This study aimed to gain insight in the determinants of online privacy protection behavior with privacy beliefs, social norms and internet skills as leading roles. A total of 23 hypotheses were tested of which 12 are supported and 4 partially supported. The next paragraphs will elaborate on the findings in order of importance. First, the role of privacy beliefs will be discussed. Then the role of internet skills and then the role of social norms will be discussed. Afterwards, other interesting findings will be elaborated. The limitations of the study and future directions will be discussed. Finally, a conclusion will be given.

5.1 Main findings

5.1.1 The role of privacy beliefs

How much do privacy beliefs play a role in predicting online privacy protection behavior on social network sites? All privacy beliefs play a role in determining online privacy protection behavior.

The analysis shows that online privacy concern has the greatest relationship with online privacy protection behavior among all determinants. The relation between privacy concern and online privacy protection behavior is in line with other literature (Child & Starcher, 2016; Dinev, Hart & Mullen, 2008; Litt, 2013; Mohamed & Ahmad, 2012; Utz & Kramer, 2009). Perceived vulnerability has a direct relationship with online privacy concern (Dinev & Hart, 2004; Mohamed & Ahmad, 2012; Yuon, 2009). Privacy disposition and perceived severity show an indirect relationship with online privacy protection behavior. A higher privacy disposition leads to higher online privacy concern (Li, 2014[a]; Li, 2014[b]; Yao et al., 2007) and a higher perceived severity. Perceived severity also relates positively to perceived vulnerability (Wang et al., 2016) and online privacy concern (Lwin et al., 2012; Mohamed & Ahmad, 2012). Perceived vulnerability also positively relates to online privacy (Dinev and Hart, 2004; Mohamed & Ahmad 2012).

Based on the results, online privacy concerns are the most important determinants of online privacy protection behavior on social network sites. Persons who feel more concerned on social network sites are more likely to take more measures in order to protect their privacy. People who feel they are more likely to become victims of online threats are more likely to be concerned and more likely to use protective measures. A person who has a higher disposition to privacy is more likely to have more online privacy concern and is more likely to experience threats as more serious. And when people experience threats as more serious, they will feel more vulnerable online and have more online privacy concerns.

In conclusion, privacy beliefs play a big role in determining online privacy protection behavior on social network sites. Persons who believe in the importance of privacy, and perceive themselves as vulnerable online due to the lack of privacy are more likely to protect themselves on social network sites. A person who has more online privacy concerns and feels more vulnerable on social network sites will take more measures to avoid becoming victims of online threats and decrease their concerns to a minimum. Online privacy concern and the perceived seriousness of privacy threats are determined by a person's disposition to privacy which means that someone's values about privacy in general plays an important role in determining concerns. Privacy disposition is often seen as a characteristic or personality trait (Li, 2014^a; Li, 2014^b), which means that someone's personality plays a role in determining online privacy protection behavior. Some persons are in general less concerned about general privacy issues than others and therefore do not use privacy protection behavior. This could be partially explained by demographic differences. Even though this study did not include the effects of gender and education, other studies have found effects of education level (Li, 2014^1) and gender (Fogel & Nehmad, 2009, Feng & Xie, 2014, Litt, 2013) on online privacy concern. Maybe there are differences in privacy disposition due to demographic differences as well.

In order to increase people's privacy on social network sites, this study advices to inform people about the possible negative outcomes of not using protection on social network sites and the severity of these possible outcomes. Many people might already be aware of the possible negative outcomes but might not understand the magnitude of these problems, or they do understand and do not care. Showing people possible negative outcomes could help them form their own opinion and position towards privacy. People's opinion of online concerns often lack firm foundation (Baek, 2014), thus presenting people with good arguments would increase their knowledge. When people are properly informed, they can decide for themselves whether they would like to protect their privacy on SNS.

5.1.2 The role of internet skills

How much do internet skills play a role in determining online privacy protection behavior on social network sites? Internet skills play a role to a certain extent in determining online privacy protection behavior on social network sites. Only social skills play an important role. In contrast to the expectations; operational skill, information navigation skill and creative skill do not play a role.

The results show that social skills are the only internet skills that show a positive relation with online privacy protection behavior on SNS. Social skill is the greatest determinant of online privacy protection behavior after online privacy concern. Other studies validate the role of social skill; online privacy skill which resembles the construct social skill, positively influences social privacy behavior such as restricting access to certain segments of information on social network profiles (Bartsch and Dienlin, 2016). Additionally, knowing how to use privacy tools increases the usage of them (Debatin, Lovejoy, Horn & Hughes, 2009).

Based on the results, people with a higher level of social skill are more likely to use online privacy protection behavior on social network sites. Thus, understanding what is perceived appropriate online behavior, knowing with whom to share your information with and understanding how privacy tools work increases the actual protection behavior. This study teaches us to acknowledge that some people might not be able to protect themselves. People need to have a certain amount of social skill since privacy beliefs alone might not be enough for people to start using online privacy protection behavior on social network sites.

Because self-efficacy can be seen as perceived internet skills (Helsper & Eynon, 2013), the role of self-efficacy will be elaborated here as well. Self-efficacy is a very strong direct determinant of internet skills. All the four internet skills, operational skill, information navigation skill, social skill and creative skill have a positive relation with self-efficacy. Prior studies confirm the impact of self-efficacy on internet skills (Broos & Roe, 2006; Hatlevik, Guomundsdottir & Loi, 2015; Zhong, 2011). Self-efficacy indirectly relates positive to privacy protection behavior due to the mediating effect of social skill.

This means that self confidence to use internet increases actual internet skills and in turn increases online privacy protection behavior due the mediating effect of social skill. Persons with a high self-efficacy are more likely to perform a certain behavior and learn while performing it (Bandura, 1991). A person who is nervous to use internet applications is less likely to use them, and therefore is less likely to learn how it works. Not having the confidence to use internet applications can cause a social inequality; this could apply on social network sites as well. People are not equally skilled in their internet skills which lead to different behaviors online. The accessibility of internet applications such as the privacy mechanisms on SNS should be made lower for people who can't keep up with the technological advances to motivate them to use these technologies. People who want to protect their privacy should be able to do so without difficulties. There are applications that can change privacy settings for people to their own preferences without much trouble. These applications are a great tool for people who do not know how to do it themselves. However, it would be more desirable of people could do it themselves.

In order to increase people's protection behavior on SNS, this study advices policy makers and teachers to focus on the use of the privacy tools, the awareness of audiences and the appropriateness of online content. Teaching people these skills might lead to more protective behaviors. When teaching people internet skills, their self-efficacy in using internet will amplify and in turn increase their skills only more which lead to more protective behaviors.

3.1.3 THE ROLE OF SOCIAL NORMS

How much do social norms play a role in determining online privacy protection behavior on social network sites? Social norms play a very small indirect role in determining online privacy protection behavior.

The results show a small indirect relation between subjective norm and online privacy protection behavior. This is in contrast to other studies that found a direct relation between the subjective norm and online privacy protection behavior (Taneja et al., 2014; Zlatolas et al., 2015). Subjective norm is the least important determinant of online privacy protection behavior. However, there is a direct relationship between subjective norm and online privacy concern and subjective norm and perceived severity.

In conclusion, the social norms play a role in people's online privacy concerns and perceived severity. When a person has more online privacy concerns and perceives problems more harmful it is more likely that they talk about it with peers increasing the subjective norm. The online privacy concerns and the perceived severity could also be higher due to the opinions of peers and the opinions of peers could also reinforce their own opinions. However, the role it plays on online privacy protection behavior is very small. People are rather independent when it comes to online privacy protection behavior on SNS. Privacy beliefs and social skills have a much larger role in determining online privacy protection behavior which means that the opinion of friends and family have not that much effect on protection behavior in comparison to someone's own privacy beliefs and their social skills.

Other literature might explain the small role of social norms on online privacy protection behavior. People are strongly biased about online privacy risks and judge themselves significantly less vulnerable to online risks than they judge others to the same risks (Cho et al., 2010). According to Zhou and Li (2014), social norm influences the usage of social network sites but not the usage of protection strategies. That is probably because people can see other people's updates when they do not protect their profiles. It is hard to acknowledge someone using privacy protection behavior because it would be protected and therefore not be seen.

3.1.4 Other findings

The results show other interesting findings. First, response efficacy positively relates to social skill. This means that when people believe in the effectiveness of privacy protection behavior, their social skill increase. It could be explained that when people believe in the effectiveness of protective behavior, they might use it more which in turn increases their skills due to the experience. However, in contrast with prior studies (Chenoweth et al., 2009; Lai et al., 2012; Lee et al., 2008; Lwin et al., 2012; Woon et al., 2005) response efficacy negatively relates with online privacy protection behavior. Maybe acknowledging the effectiveness of online privacy protection behavior is part of people's social skill and there might be a gap between the perceived effectiveness of online privacy protection behavior and the actual effectiveness of online privacy protection behavior on social network sites. Some people believe that companies and schools can bypass privacy settings on SNS and therefore don't believe in the effectiveness of protection tools (Moreno, Kelleher, Ameenuddin & Rastogi, 2014). Maybe people believe that there is almost no privacy left on SNS and therefore stopped taking actions about it. This gap could explain why some people don't protect themselves on SNS. Closing this gap and educating people about the actual efficacy of privacy settings on SNS might lead to more protective behaviors. Additionally, a higher response efficacy leads to lower levels of online privacy concern, which can be explained that when people feel using protective measures are effective in protecting themselves from privacy loss, their online privacy concern decreases (Xu, Dinev, Smith & Hart, 2008).

Furthermore, social skill negatively relates with perceived vulnerability. Thus, people with a higher level of social skill feel less vulnerable on SNS. This could be explained with people with higher level of social skill are using more protection behavior which in case decreases their perceived vulnerability, it is more difficult for people to misuse content when it is less available. Another explanation is that people with more social skills might feel less vulnerable due to their own perception of their ability to handle possible threats.

Operational skill negatively relates with subjective norm. This could be explained with that people with higher operational skills might have more faith in themselves regarding their online skills than they value the opinions of others. Or, people with a high level of operational skills might talk less about online problems because they experience fewer problems due to their own skills. Therefore, they might be less subjected to social norms.

5.2 Limitations and future directions

This study has a couple limitations that will be addressed and may be improved in future studies. First, the privacy disposition and subjective norm was measured with a 2-item scale. During the pre-test the scale turned out to be sufficient but in the final survey, the items were dropped due to a low internal consistency. Even though the alpha was still sufficient it would have been better to measure it with a 3-item scale.

The participants of the study were fairly high educated in comparison to the Dutch population which makes the generalizability to the Dutch population low. This could also jeopardize some results, especially the results of the internet skills since other studies have found out that there are significant differences in internet skills due to a person's education level and/or social-economic status (Van Deursen & Van Dijk, 2010). For example: the operational skills showed a very high value with a low standard deviation which means that there was not much variance in the construct. Also, socio-demographic variables affect the levels of privacy concern (Cecere, Guel & Soulié, 2015).

It is important to consider that self-reported behavior is different than observed behavior. What people say is sometimes in contrast with what they actually do to protect their online privacy (Jensen, Potts & Jensen, 2005). Some people have wrong perceptions about their own knowledge about privacy issues and their vulnerabilities online (Jensen et al., 2005; Moll et al., 2014). So, persons could claim they have internet skills or use protection techniques while in fact they are not as protected or skilled as they think they are. Additionally, while measuring skills, people tend to overestimate themselves. People with higher self-reported levels of internet skills do not always show actual higher levels of observed internet skills (Zhong, 2011). People might show different behavior in real life than they say in survey studies. However, this is a limitation which is hard to tackle when using a survey. Unobtrusive studies on online privacy protection behavior in combination with experiments to measure someone's skills might be an opportunity for future studies.

This study focused on SNS in general. There might be differences in the behavior of people on different SNS. For example, people have more sense of trust in Facebook than MySpace (Fogel & Nehmad, 2009). The reason why someone uses SNS might also be important in predicting online privacy behaviors. A person searching for a date might have more public profiles than someone who feels he has enough friends and does not want strangers to look into their profiles.

The reasons why people protect themselves on SNS are probably different than when people protect themselves from data collection in general. People on SNS might try to protect their privacy from stalkers or scam artists while people who try to protect their tracking data have different motives. In the case of protecting yourself from scam artists, the privacy tools of SNS are efficient, but in protecting yourself from data collection, the privacy tools are not sufficient. Maybe therefore people do not find the privacy mechanisms effective in protecting their privacy. This study did not distinguish these different dimensions of privacy intrusion in the construct of response efficacy. The reason and nature of this gap might be a great opportunity for future studies.

Privacy concerns and someone's privacy disposition could derive from many different reasons which do not fit in quantitative studies. People could have seen other people's privacy being invaded or experienced privacy intrusive problems themselves. Maybe people are getting more and more annoyed by spam and advertisements or maybe some people have disclosed more information online and feel more need to protect their information. Maybe they have more skills and are more aware of online problems, or maybe they watch more privacy related news. This study and many other studies do not explain all the reasons why. So there is a gap that could be filled with qualitative studies.

Another interesting study might be how internet skills influence someone's privacy disposition or vice versa. There was a negative correlation found between privacy disposition and information navigation skills. The subject is not yet elaborated and discussed in depth. Why and how privacy disposition links with information navigation skills might be an opportunity for future studies.

5.3 Conclusion

This study increases our understanding in the online privacy protection behavior of people and the results can be used by governments, teachers or other individuals to improve online safety on SNS. *What is the role of privacy beliefs, social norms and internet skills on online privacy protection behavior on SNS?* Privacy beliefs have the greatest role in predicting online privacy protection behavior on social network sites. Especially online privacy concern and perceived vulnerability. Social skills are the only necessary internet skills in order for people to protect their online privacy on social network sites and social norms have a very small indirect role in determining online privacy protection behavior on social network sites.

Future studies on privacy behavior should also include the effect of social skills since beliefs and attitudes are not sufficient in predicting online privacy protection behavior on SNS. There might be a gap in the perceived effectiveness of online privacy protection behavior and the actual effectiveness of online privacy protection behavior on SNS which deserves more attention in future studies.

6. REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32(4), 665-683.

Baek, Y.M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior,* 38, 33-42.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review,* 84(2), 191-215.

Bandura, A. (1989). Regulation of cognitive processes through perceived self-efficacy. *Developmental Psychology*, 25(5), 729-735.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes,* 50(2), 248-287.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior,* 56, 147-154.

boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. *Networked Self: Identity, Community, and Culture on Social Network Sites*, 39-58.

Broos, A., & Roe, K. (2006). The digital divide in the playstation generation: Self-efficacy, locus of control and ICT adoption among adolescents. *Poetics,* 34(4), 306-317.

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Media Change,* 96, 277-287.

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In Proceedings of the 42nd Hawaii international conference on system sciences, 1–10.

Child, J.T., & Starcher, S.C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior,* 54, 483-490.

Cho, H., Lee, J.S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior,* 26, 987-995.

Crossler, R. E. (2010). Protection motivation theory: understanding determinants to backing up personal data. In Proceedings of the 43rd Hawaii international conference on system sciences, 1–10.

Debatin, B., Lovejoy, J.P., Horn, A.K., & Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication,* 15(1), 83-108.

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

Dinev, T., & Hart, P. (2006). Internet privacy concerns and social awareness as determinants of intention to transact*. International Journal of Electric Commerce,* 10(2), 7-29.

Dinev T., Hart, P., & Mullen, M.R. (2008). Internet privacy concerns and beliefs about government surveillance – an empirical investigation. *Journal of Strategic Information Systems,* 17, 214-233.

Eastin, M.S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of Computer Mediated Communication,* 6(1).

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, 33, 153-162.

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

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), 263-272.

Hattlevik, O.E., Guomundsdottir, G.B., & Loi, M. (2015). Digital diversity among upper class secondary students: A multilevel analysis of the relationship between cultural, self-efficacy, strategic use of information and digital competence. *Computers and Education,* 81, 345-353.

Hattlevik, O.E., Ottestad, G., & Throndsen, I. (2014). Predictors of digital competence in 7th grade: A multilevel analysis. *Journal of Computer Assisted Learning,* 31(3), 220-231.

Helsper, E., & Eynon, R. (2013). Distinct skill pathways to digital engagement*. European Journal of Communication*, 28 (6).

Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47, 154-165.

Hofstra, B., Corten, R., van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior,* 60, 611-621.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies,* 63, 203-227.

Kurt, M. (2010). Determination of in internet privacy behaviors of students. *Procedia-Social and Behavioral Sciences,* 9, 1244-1250.

Lai, F., Li, D., & Hsieh, C.T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems,* 52, 353-363.

Lee, D., LaRose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication,* 14(1), 79-100.

Li, Y. (2014^{a}). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications,* 13(1), 32-44.

Li, Y. (2014^{b}). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems,* 57, 343-354.

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

Lwin, M.O., Li, B., & Ang, R.P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence,* 35(1), 31-41.

Mohamed, N., & Ahmad, I.H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior,* 28(6), 2366-2375.

Moll, R., Pieschl, S., & Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior,* 41, 212-219.

Moreno, M.A., Kelleher, E., Ameenuddin, N., & Rastogi, S. (2014). Young adult females' views regarding online privacy protection at two time points. Journal of Adolescent Health, (55), 347-351.

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior,* 49, 324-332.

Paine, C., Reips, U., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies,* 65(6), 526-536.

Park, Y.J. (2011). Digital literacy and privacy behavior online. *Communication Research,* 40(2), 215-236.

Park, Y.J., Campbell, S.W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior,* 28(3), 1019-1027.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. *Pew Research Center,* from http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Rosdorff, M. (2016, April 8). Twee nieuwe voorbeelden van fraude via social media. Retrieved May 17, 2016, from http://trendingvandaag.eenvandaag.nl/items/66385/twee_nieuwe_voorbeelden_van_fraude_via_social_media

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114.

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

Taneja, A., Vitrano, J., & Gengo, N.J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior,* 38, 159-173.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., & Cotten, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security,* 59, 138-150.

Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2), article 1. From: http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

Van Deursen, A.J.A.M., Helsper, E.J., & Eynon, R. (2015). Development and validation of the internet skills scale (ISS). *Information, Communication & Society.*

Van Deursen, A.J.A.M., & Van Dijk, J.A.G.M. (2010) Internet skills and the digital divide. *New Media & Society,* XX(X), 1-19.

Wang, T., Duong, T.D., & Chen, C.C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management,* 36, 531-542.

Westin, A.F. (2003). Social and political dimensions of privacy. *Journal of Social Issues,* 59(2), 1-37.

Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in facebook. *Computers in Human Behavior,* 35, 444-454.

Woon, I., Tan, G.W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In Proceedings of the 26th International Conference on Information Sytems. Las Vegas, Nevada, USA. Paper 31.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In International conference on information systems. Paris, France. ICIS 2008 Proceedings. Paper 6. http://aisel.aisnet.org/icis2008/6

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information System,* 12(12), 798-824.

Yao, M.Z., Rice, R.E. & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology,* 58(5), 710-722.

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

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3),180–197.

Zhong, Z.J. (2011). From access to usage: The divide of self-reported internet skills among adolescents. *Computers & Education,* 56(3), 736-746.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior,* 37, 283-289.

Zlatolas, L.N., Welzer, T., Hericko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior,* 45, 158-167.

APPENDICES

A. PRE-TESTED ITEMS AND REMAINING ITEMS

Online Privacy Protection Behavior

Pre-tested items	Remaining items after pre-test α = .76 (Definitive survey)
Feng & Xie (2014)	
1) I sometimes delete people from my network or friends' list.	1) I sometimes delete people from my network or friends' list.
2) I sometimes remove my name from photos that I have been tagged on.	2) I sometimes remove my name from photos that I have been tagged on.
3) I sometimes delete comments that others have made on my profiles or accounts.	3) I sometimes delete comments that others have made on my profiles or accounts.
4) Sometimes, I delete or edit something that I posted in the past.	4) Sometimes, I delete or edit something that I posted in the past.
5) I sometimes post fake information like a fake name, age or location to help protect my privacy.	5) I rarely block people. (reverse-worded) 6) I often use the privacy-settings to set the visibility of my profile and online posts to friends only.
6) I rarely block people. (reverse-worded)	
7) I rarely delete or deactivate social network profiles or accounts. (reverse-worded)	
Author added items	
8) I often use the privacy-settings to set the visibility of my profile and online posts to friends only.	
9) I sometimes encrypt my online messages so that only my friends understand what I am talking about.	
10) I sometimes withhold from posting something online after I thought about it for a second time.	

Online Privacy Concern

Pre-tested items	Remaining items after pre-test α = .89 (Definitive survey)
Zlatolas, Welzer, Hericko &Hölbl (2015)	
1) It bothers me when I have to put much personal information on SNSs.	1) It bothers me when I have to put much personal information on SNSs.
2) I am concerned that SNSs are collecting too much personal information about me.	2) I am concerned that SNSs are collecting too much personal information about me.
3) I am concerned that unauthorized people could access my personal information.	3) I am concerned that unauthorized people could access my personal information.
4) I am concerned that SNSs use my personal information for purposes that I am not being notified of.	4) I am concerned that SNSs use my personal information for purposes that I am not being notified of.
5) I am concerned when I have to post personal information on SNSs.	

Privacy Disposition

Pre-tested items	Remaining items after pre-test α = .96 (Definitive survey)
Li (2014) 1) Compared to others, I am more concerned about the way other people or organizations handle my personal information. 2) Compared to others, I see more importance in keeping personal information private. 3) Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)	1) Compared to others, I am more concerned about the way other people or organizations handle my personal information. 2) Compared to others, I see more importance in keeping personal information private. 3) Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)

Perceived Vulnerability

Pre-tested items	Remaining items after pre-test α = .8 (Definitive survey)
How likely do you think these issues will happen to you? *Lwin, Li & Ang (2012)* 1) Receiving hate emails. 2) Being threatened online. 3) Receiving unpleasant sexual remarks online. 4) Someone pretending to be me online. 5) Someone publishing my personal information online with bad intentions. 6) Someone posting my personal photos/videos online with the intention to harm me. 7) Someone posting negative rumors or inflammatory remarks about me online. *Dinev & Hart (2004)* 8) My personal information being made available to the government. 9) My personal information being made available to unknown companies or persons.	1) Receiving hate emails. 2) Being threatened online. 3) Someone publishing my personal information online with bad intentions. 4) My personal information being made available to the government. 5) My personal information being made available to unknown companies or persons.

Perceived Severity

Pre-tested items	Remaining items after pre-test α = .83 (Definitive survey)
How serious are these issues to you? *Lwin, Li & Ang (2012)* 1) Receiving hate emails. 2) Being threatened online. 3) Receiving unpleasant sexual remarks online. 4) Someone pretending to be me online. 5) Someone publishing my personal information online with bad intentions. 6) Someone posting my personal photos/videos online with the intention to harm me. 7) Someone posting negative rumors or inflammatory	1) Receiving hate emails. 2) Being threatened online. 3) Someone publishing my personal information online with bad intentions. 4) My personal information being made available to the government. 5) My personal information being made available to unknown companies or persons.

remarks about me online. *Dinev & Hart (2004)* 8) My personal information being made available to the government. 9) My personal information being made available to unknown companies or persons.	

Subjective Norm

Pre-tested items	Remaining items after pre-test α = .82 (Definitive survey)
Zlatolas, Welzer, Hericko &Hölbl (2015)	
1) People who have influence on me believe that it is not very important to keep my personal information private. (reverse-worded) 2) Important friends believe that I need to take care about my privacy. 3) People who are important to me believe that I should be careful with exposing my information online.	1) People who have influence on me believe that it is not very important to keep my personal information private. (reverse-worded) 2) Important friends believe that I need to take care about my privacy. 3) People who are important to me believe that I should be careful with exposing my information online.

Self-Efficacy

Pre-tested items	Remaining items after pre-test α = .87 (Definitive survey)
Yao, Rice, & Wallis (2007)	
1) Normally I know how to solve problems online. 2) Normally I get what want online. 3) Normally I stick to my aims/goals online 4) I am confident in unexpected events online. 5) I am resourceful in unforeseen situations online. 6) I solve problems when necessary with not much effort online. 7) I get nervous when I have problems online. (reverse-worded) 8) Normally I can find several solutions online. 9) When I am in trouble online, I normally can think of a solution. 10) I normally can handle whatever online problem that comes my way.	1) I get nervous when I have problems online. (reverse-worded) 2) Normally I can find several solutions online. 3) When I am in trouble online, I normally can think of a solution. 4) I normally can handle whatever online problem that comes my way.

Response Efficacy

Pre-tested items	Remaining items after pre-test α =.72 (Definitive survey)
Mohamed & Ahmad (2012)	
1) I can protect my information privacy better if I use privacy protection measures in social networking sites. 2) Utilizing privacy protection measures in social networking sites don't work to ensure my information privacy. (reverse-worded)	1) I can protect my information privacy better if I use privacy protection measures in social networking sites. 2) Using privacy settings on social networking sites makes me less likely to lose my information

3) If I utilize privacy protection measures in social networking sites, unknown people are less likely to gain access to my information. *Lwin, Li & Ang (2012)* 4) If I used privacy protection measures in social network sites, I could prevent myself from being bullied online. 5) I am less prone to be a victim of harassment if I limit access to my profile to friends only. *Author added items* 6) If I used privacy protection measures in social networking sites, I could probably protect myself from online threats. 7) Using privacy settings on social networking sites makes me less likely to lose my information privacy. 8) Using privacy settings on social network sites are beneficial to my privacy. (Authors own input) 9) Privacy settings on social network sites do not help protecting my privacy. (reverse-worded)(Authors own input)	privacy. 3) Using privacy settings on social network sites are beneficial to my privacy. 4) Privacy settings on social network sites do not help protecting my privacy. (reverse-worded)

Operational Skill

Pre-tested items	**Remaining items after pre-test α = .76 (Definitive survey)**
Van Deursen, Helsper & Eynon (2015) 1) I know how to open downloaded files. 2) I know how to download/save a photo I found online. 3) I know how to use shortcut keys. 4) I know how to open a new tab in my browser. 5) I know how to bookmark a website. 6) I know how to upload files. 7) I know how to adjust privacy settings	1) I know how to download/save a photo I found online. 2) I know how to open a new tab in my browser. 3) I know how to bookmark a website. 4) I know how to upload files.

Information Navigation Skill

Pre-tested items	**Remaining items after pre-test α = .76 (Definitive survey)**
Van Deursen, Helsper & Eynon (2015) 1) I find it easy to decide what the best keywords are to use for online searches. (reverse-worded) 2) I find it hard to find a website I visited before. 3) I get tired when looking for information online. 4) Sometimes I end up on websites without knowing how I got there. 5) I find the way in which many websites are designed confusing. 6) All the different website layouts make working with the internet difficult for me. 7) Sometimes I find it hard to verify information I have retrieved.	1) I find it easy to decide what the best keywords are to use for online searches. (reverse-worded) 2) I find the way in which many websites are designed confusing. 3) All the different website layouts make working with the internet difficult for me. 4) Sometimes I find it hard to verify information I have retrieved.

Social Skill

Pre-tested items	Remaining items after pre-test α = .77 (Definitive survey)
Van Deursen, Helsper & Eynon (2015)	
1) I know which information I should and shouldn’t share online.	1) I know which information I should and shouldn’t share online.
2) I know when I should and shouldn’t share information online.	2) I know when I should and shouldn’t share information online.
3) I am careful to make my comments and behaviors appropriate to the situation I find myself in online.	3) I know how to change who I share content with (e.g. friends, friends of friends or public).
4) I know how to change who I share content with (e.g. friends, friends of friends or public).	4) I know how to change my privacy-settings.**(from operational skills)**
5) I don’t know how to remove friends from my contact lists. (reverse-worded)	
6) I feel comfortable deciding who to follow online (e.g. on services like Twitter or Tumblr).	

Creative Skill

Pre-tested items	Remaining items after pre-test α = .85 (Definitive survey)
Van Deursen, Helsper & Eynon (2015)	
1) I know how to create something new from existing online images, music or video.	1) I know how to create something new from existing online images, music or video.
2) I know how to make basic changes to the content that others have produced.	2) I know how to make basic changes to the content that others have produced.
3) I don’t know how to design a website.(reverse-worded)	3) I don’t know how to design a website.(reverse-worded)
4) I know which different types of licenses apply to online content.	4) I know which different types of licenses apply to online content.
5) I would feel confident putting video content I have created online.	
6) I am confident about writing a comment on a blog, website or forum.	

B. Demographic survey items

Demographics

Construct	Items	Answer methods
Gender	What is your gender?	Male/female
Education	What is your highest finished education?	Primary school Middle School MBO HBO University
Age	What is your age?	Open

Demographics - Translations

Construct	Items	Answer methods
Geslacht	Wat is je geslacht?	Man/Vrouw
Opleidingsniveau	Wat is je hoogste genoten opleiding?	Basisschool Middelbareschool MBO HBO Universiteit
Leeftijd	Wat is je leeftijd?	Open

C. Introduction to respondents before survey

Beste Respondent,

Bedankt dat u mee wilt doen aan dit onderzoek.

Deze enquête maakt deel uit van mijn afstudeeronderzoek over privacy gedrag op sociale netwerken. Denk hierbij aan Tumblr, Twitter, Instagram, Facebook en dergelijke.

Uw mening, gevoelens en houding met betrekking tot privacy zullen worden gevraagd. Het is belangrijk dat u de vragenlijst zo eerlijk en volledig mogelijk invult. Er zijn geen goede of foute antwoorden.

Het invullen van deze enquête duurt ongeveer 10 minuten. Dit onderzoek is compleet anoniem en uw gegevens zullen vertrouwelijk behandeld worden. De resultaten zullen alleen worden gebruikt voor academische doeleinden. U kunt u te allen tijden zonder rechtvaardiging of verklaring terugtrekken.

Ik heb begrepen waar dit onderzoek over gaat en ik stem in dat mijn antwoorden uitsluitend gebruikt worden ten behoeve van dit onderzoek. (Checkbox)

Nogmaals bedankt voor uw medewerking!

Met vriendelijke groet,

Maarten van der Kamp

Master Student Communication Studies, Universiteit Twente

D. Translations survey-items

Item Translations English - Dutch

Items	Dutch translations
Online Privacy Protection Behavior	
1) I sometimes delete people from my network or friends' list. 2) I sometimes remove my name from photos that I have been tagged on. 3) I sometimes delete comments that others have made on my profiles or accounts. 4) Sometimes, I delete or edit something that I posted in the past. 5) I sometimes post fake information like a fake name, age or location to help protect my privacy. 6) I rarely block people. (reverse-worded) 7) I rarely delete or deactivate social network profiles or accounts. (reverse-worded) 8) I often use the privacy-settings to set the visibility of my profile and online posts to friends only. 9) I sometimes encrypt my online messages so that only my friends understand what I am talking about. 10) I sometimes withhold from posting something online after I thought about it for a second time.	1) Ik verwijder wel eens mensen uit mijn sociale netwerken. 2) Ik verwijder mijzelf wel eens van foto's waar ik in getagt ben. 3) Ik verwijder wel eens commentaren van anderen op mijn profiel. 4) Soms verwijder of pas ik berichten aan die ik in het verleden gemaakt heb. 5) Ik gebruik wel eens valse informatie (zoals naam, leeftijd of locatie) om mijn privacy te beschermen. 6) Ik blokkeer zelden mensen op mijn sociale netwerken. 7) Ik verwijder of deactiveer zelden mijn sociale netwerk accounts. 8) Ik gebruik meestal privacy settings om mijn profiel en berichten zichtbaar te maken voor alleen vrienden. 9) Ik gebruik soms geheimtaal in mijn online berichten die alleen mijn vrienden kennen. 10) Ik weerhoud mijzelf er soms van iets online te plaatsen nadat ik er voor de tweede keer over heb nagedacht.
Online Privacy Concern	
1) It bothers me when I have to put much personal information on SNSs. 2) I am concerned that SNSs are collecting too much personal information about me. 3) I am concerned that unauthorized people could access my personal information. 4) I am concerned that SNSs use my personal information for purposes that I am not being notified of. 5) I am concerned when I have to post personal information on SNSs.	1) Het stoort me wanneer ik veel persoonlijke informatie moet opgeven op sociale media. 2) Ik ben bezorgd dat sociale media te veel persoonlijke informatie van mij verzamelen. 3) Ik ben bezorgd dat ongeoorloofde mensen mijn persoonlijke informatie kunnen bekijken. 4) Ik ben bezorgd dat sociale media. mijn persoonlijke informatie gebruiken voor doelen waar ik geen weet van heb. 5) Ik raak bezorgd wanneer ik persoonlijke informatie op sociale media. moet posten.
Privacy Disposition	
1) Compared to others, I am more concerned about the way other people or organizations handle my personal information. 2) Compared to others, I see more importance in keeping personal information private. 3) Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)	1) In vergelijking met anderen ben ik bezorgd over de manier waarop bedrijven en mensen met mijn persoonlijke informatie omgaan. 2) In vergelijking met anderen zie ik meer belang in het privé houden van persoonlijke informatie. 3) In vergelijking met anderen ben ik minder bezorgd over potentiële bedreigingen van mijn privacy.
Perceived Vulnerability	
How likely do you think these issues will happen to you? 1) Receiving hate emails. 2) Being threatened online. 3) Receiving unpleasant sexual remarks online.	*Hoe groot acht je de kans dat je slachtoffer wordt van de volgende zaken?* 1) Ontvangen van haat e-mails. 2) Online bedreigd worden. 3) Online ongewenste seksuele opmerkingen

4) Someone pretending to be me online. 5) Someone publishing my personal information online with bad intentions. 6) Someone posting my personal photos/videos online with the intention to harm me. 7) Someone posting negative rumors or inflammatory remarks about me online. 8) My personal information being made available to the government. 9) My personal information being made available to unknown companies or persons.	ontvangen. 4) Iemand die zich voordoet als mij online. 5) Iemand die persoonlijke informatie van mij online zet met verkeerde bedoelingen. 6) Iemand die persoonlijke foto’s/video’s van mij online zet met de intentie mij te beschadigen. 7) Iemand die negatieve roddels over mij verspreid online. 8) Dat mijn persoonlijke informatie beschikbaar wordt gemaakt voor de overheid. 9) Dat mijn persoonlijke informatie beschikbaar wordt gemaakt voor onbekende personen of bedrijven.
Perceived Severity	
How serious are these issues to you? 1) Receiving hate emails. 2) Being threatened online. 3) Receiving unpleasant sexual remarks online. 4) Someone pretending to be me online. 5) Someone publishing my personal information online with bad intentions. 6) Someone posting my personal photos/videos online with the intention to harm me. 7) Someone posting negative rumors or inflammatory remarks about me online. 8) My personal information being made available to the government. 9) My personal information being made available to unknown companies or persons.	Hoe serieus zijn de volgende zaken voor je? 1) Ontvangen van haat e-mails. 2) Online bedreigd worden. 3) Online ongewenste seksuele opmerkingen ontvangen. 4) Iemand die zich voordoet als mij online. 5) Iemand die persoonlijke informatie van mij online zet met verkeerde bedoelingen. 6) Iemand die persoonlijke foto’s/video’s van mij online zet met de intentie mij te beschadigen. 7) Iemand die negatieve roddels over mij verspreid online. 8) Dat mijn persoonlijke informatie beschikbaar wordt gemaakt voor de overheid. 9) Dat mijn persoonlijke informatie beschikbaar wordt gemaakt voor onbekende personen of bedrijven.
Subjective Norm	
1) People who have influence on me believe that it is not very important to keep my personal information private. (reverse-worded) 2) Important friends believe that I need to take care about my privacy. 3) People who are important to me believe that I should be careful with exposing my information online.	1) Mensen die invloed op mij hebben vinden het niet heel belangrijk om persoonlijke informatie privé te houden. 2) Belangrijke vrienden vinden dat ik moet zorgen dat ik mijn privacy waarborg. 3) Mensen die belangrijk voor mij zijn vinden dat ik voorzichtig moet zijn met informatie online zetten.
Self-Efficacy	
1) Normally I know how to solve problems online. 2) Normally I get what want online. 3) Normally I stick to my aims/goals online 4) I am confident in unexpected events online. 5) I am resourceful in unforeseen situations online. 6) I solve problems when necessary with not much effort online. 7) I get nervous when I have problems online. (reverse-worded) 8) Normally I can find several solutions online. 9) When I am in trouble online, I normally can think of a solution. 10) I normally can handle whatever online problem that comes my way.	1) Normaal gesproken weet ik hoe ik problemen op het internet moet oplossen. 2) Normaal gesproken krijg ik wat ik wil online. 3) Normaal gesproken blijf ik bij mijn doelen online. 4) Ik ben zelfverzekerd in onverwachte situaties online. 5) Ik weet wat ik moet doen in onvoorziene situaties online. 6) Ik los online problemen op met weinig moeite. 7) Ik word nerveus wanneer ik online problemen heb. 8) Normaal gesproken vind ik meerdere oplossingen online. 9) Wanneer ik in de problemen zit op het internet,

	vind ik vaak een oplossing. 10) Normaal gesproken kan ik de meeste problemen oplossen die online ontstaan.
Response Efficacy	
1) If I used privacy protection measures in social networking sites, I could probably protect myself from online threats. 2) If I used privacy protection measures in social network sites, I could prevent myself from being bullied online. 3) I am less prone to be a victim of harassment if I limit access to my profile to friends only. 4) I can protect my information privacy better if I use privacy tools in social networking sites. 5) Utilizing privacy protection measures in social networking sites don't work to ensure my information privacy. (reverse-worded) 6) If I utilize privacy protection measures in social networking sites, unknown people are less likely to gain access to my information. 7) Using privacy settings on social networking sites makes me less likely to lose my information privacy. 8) Using privacy settings on social network sites are beneficial to my privacy. (Authors own input) 9) Privacy settings on social network sites do not help protecting my privacy. (reverse-worded)(Authors own input)	1) Als ik privacy beveiligingsmaatregelen neem, kan ik mijzelf beter beschermen tegen online bedreigingen. 2) Als ik privacy beveiligingsmaatregelen neem, kan ik voorkomen dat ik online gepest wordt. 3) Als ik mijn profiel alleen zichtbaar maak voor mijn vrienden is er een kleinere kans dat ik slachtoffer wordt van online intimidatie of pesterijen. 4) Ik zou mijn informatie beter kunnen beschermen als ik de privacy instellingen op mijn sociale netwerken gebruik. 5) Het gebruik maken van privacy instellingen op sociale netwerken zorgen er niet voor dat mijn privacy beschermd wordt. 6) Als ik privacy beveiligingsmaatregelen neem zullen onbekende mensen minder snel toegang hebben tot mijn persoonlijke informatie. 7) Het gebruik maken van privacy instellingen op sociale netwerken zorgen ervoor dat ik minder snel mijn persoonlijke privacy verlies. 8) Het gebruiken van privacy settings op sociale netwerken zijn gunstig voor mijn privacy. 9) Privacy settings op sociale netwerken helpen niet in het beschermen van mijn privacy.
Operational Skill	
1) I know how to open downloaded files. 2) I know how to download/save a photo I found online. 3) I know how to use shortcut keys. 4) I know how to open a new tab in my browser. 5) I know how to bookmark a website. 6) I know how to upload files. 7) I know how to adjust privacy settings.	1) Ik weet hoe ik bestanden kan downloaden. 2) Ik weet hoe ik een foto van het internet kan opslaan. 3) Ik weet hoe ik sneltoetsen kan gebruiken (bv CTRL-c voor kopie). 4) Ik weet hoe ik een nieuw venster open in mijn internet browser. 5) Ik weet hoe ik een website kan toevoegen aan de favorieten. 6) Ik weet hoe ik bestanden kan uploaden. 7) Ik weet hoe ik privacy instellingen kan aanpassen.
Information Navigation Skill	
1) I find it easy to decide what the best keywords are to use for online searches. (reverse-worded) 2) I find it hard to find a website I visited before. 3) I get tired when looking for information online. 4) Sometimes I end up on websites without knowing how I got there. 5) I find the way in which many websites are designed confusing. 6) All the different website layouts make working with the internet difficult for me. 7) Sometimes I find it hard to verify information I have retrieved.	1) Ik vind het makkelijk om te besluiten wat de beste zoekwoorden zijn. 2) Ik vind het moeilijk een website die ik eerder bezocht terug te vinden. 3) Ik vind informatie zoeken op internet vermoeiend. 4) Soms zit ik op een website zonder dat ik weet hoe ik er kwam. 5) Ik vind de manier waarop veel websites zijn ontworpen verwarrend. 6) Al de verschillende website-ontwerpen maakt internetten lastig. 7) Ik vind het soms moeilijk om gevonden informatie te controleren op juistheid.

Social Skill	
1) I know which information I should and shouldn’t share online.	1) Ik weet welke informatie ik wel of niet kan delen op internet.
2) I know when I should and shouldn’t share information online.	2) Ik weet wanneer ik informatie wel of niet kan delen op internet.
3) I am careful to make my comments and behaviors appropriate to the situation I find myself in online.	3) Ik zorg dat mijn commentaar en gedrag passen bij de situatie waarin ik mij op internet bevind.
4) I know how to change who I share content with (e.g. friends, friends of friends or public).	4) Ik weet hoe ik kan aanpassen met wie ik informatie deel (bv. vrienden, vrienden van vrienden, of iedereen).
5) I don’t know how to remove friends from my contact lists. (reverse-worded)	5) Ik weet niet hoe ik vrienden uit mijn contactlijst kan verwijderen.
6) I feel comfortable deciding who to follow online (e.g. on services like Twitter or Tumblr).	6) Ik voel me zelfverzekerd bij het beslissen wie ik volg op plaatsen waar informatie wordt gedeeld (bv. Twitter of Tumblr).
Creative Skill	
1) I know how to create something new from existing online images, music or video.	1) Ik weet hoe ik iets nieuws kan maken van bestaande online plaatjes, muziek of video’s.
2) I know how to make basic changes to the content that others have produced.	2) Ik weet hoe ik kleine aanpassingen kan maken aan materiaal dat anderen hebben gemaakt.
3) I don’t know how to design a website.(reverse-worded)	3) Ik weet niet hoe ik een website kan maken.
4) I know which different types of licenses apply to online content.	4) Ik weet welke (kopieer)rechten van toepassing zijn op online materiaal.
5) I would feel confident putting video content I have created online.	5) Ik zou me zelfverzekerd voelen bij het op internet plaatsen van zelf gemaakte video’s.
6) I am confident about writing a comment on a blog, website or forum.	6) Ik voel me zelfverzekerd bij het plaatsen van berichten op een weblog, website of forum.

E. Letter that was used to collect respondents

Beste buurtbewoner,

In het kader van mijn studie doe ik een onderzoek naar online privacy gedrag op sociale media. Denk hierbij aan Facebook, Twitter, Instagram en dergelijke. Hierbij wil ik u graag om hulp vragen. Wilt u 10 minuten de tijd nemen om mijn afstudeeronderzoek in te vullen? Het onderzoek is compleet anoniem en u zult me er enorm mee helpen.

Het onderzoek kan gemaakt worden op de pc, laptop, tablet of smartphone, via de link of via de QR-code. **Link: http://bit.ly/1RwL58a**

Heeft u vragen of bent u geïnteresseerd in het onderzoek en de uiteindelijke resultaten, dan kunt u mailen naar m.h.vanderkamp@student.utwente.nl. Met plezier zal ik uw e-mail beantwoorden.

Met vriendelijke groet,
Maarten van der Kamp