THE INFLUENCE OF RESIGNATION ON THE PRIVACY CALCULUS IN THE CONTEXT OF SOCIAL NETWORKING SITES: AN EMPIRICAL ANALYSIS

Research paper

Jakob Wirth, University of Bamberg, Germany, jakob.wirth@uni-bamberg.de

Christian Maier, University of Bamberg, Germany, christian.maier@uni-bamberg.de

Sven Laumer, Friedrich-Alexander Universität Erlangen-Nürnberg, Germany, sven.laumer@fau.de

Abstract

Individuals conduct a privacy calculus before they disclose information by weighing benefits with privacy risks of disclosure. In line with the privacy calculus, if benefits outweigh privacy risks individuals disclose information, otherwise they do not. However, research has also challenged the privacy calculus because individuals also disclose information even in light of low benefits and high privacy risks. Given explanations refer to 1) altering the perceptions of benefits and privacy risks or 2) altering the effect of benefits and privacy risks on disclosure. Whereas studies focusing on the first part have provided explanations for why the privacy calculus is sometimes not confirmed, studies on the second part do not do so. This study is therefore considering the second part and is integrating an individual's level of resignation to protect one's privacy in the context of social networking sites. We consider resignation as a reaction of individuals to given privacy threats. Results show that when including resignation the effect of benefits becomes stronger and the effect of privacy risks becomes weaker. Implications for theory include that resignation helps in explaining why individuals disclose information even when only small benefits and high privacy risks are present.

Keywords: Privacy Calculus, Resignation, Privacy Risks, Benefits.

1 Introduction

Many individuals disclose information about themselves on social networking sites (SNS), such as a profile photo or general news about their life (Boyd and Ellison 2007). Such disclosure involves benefits, e.g. having fun (Sun et al. 2015) and privacy risks, e.g. becoming a victim of identity theft (Dinev 2014). If benefits outweigh privacy risks, then individuals disclose information with the goal to take advantage of the benefits. This is called the *privacy calculus* (Dinev and Hart 2006).

Research has challenged the privacy calculus such that individuals also disclose information despite low benefits and high privacy risks (Acquisti 2004; Dinev et al. 2015). On the one hand, research has shown that this is due to a misperception of individuals of their benefits and privacy risks. Although benefits are objectively low, individuals perceive them as high. Vice versa, although privacy risks are objectively high, individuals perceive them as low. Then individuals have a high perception of benefits and a low perception of privacy risks, leading to disclosure of information. Previous research has provided several explanations for such a misperception (Acquisti 2004; Dinev et al. 2015).

On the other hand, the strength of the *effect* of benefits and privacy risks on disclosure can also lead to individuals disclosing information despite low benefits and high privacy risks (Brakemeier et al. 2016). Previous research has shown that perceptions (Sarathy and Li 2007; Sun et al. 2015; Xu et al. 2003) and

mental states (Brakemeier et al. 2016) of individuals may alter the effect of benefits and privacy risk on disclosure.

However, although these concepts have helped furthering our understanding of the privacy calculus, they do not help to explain why individuals disclose information despite low benefits and high privacy risks. Additional concepts altering the effect of benefits and privacy risks on disclosure might be more useful to provide such an explanation. Previous research indicates that reactions of individuals to certain events could be such a concept (Cicchetti 2016; Ortiz de Guinea and Webster 2013; Pirkkalainen et al. 2017; Rogers and Prentice-Dunn 1997). One such reaction is *resignation* which is a reaction of individuals to given events such as threats where individuals accept that threat and show no signs of changing it (Feifel and Strack 1989). Anecdotal evidence indicates that in the context of privacy, individuals have resigned by accepting privacy threats and by having the perception that they cannot change these privacy threats (Lee and Maeve 2016; Morgan 2014). Previous research has additionally indicated that resignation could alter the effect of benefits and privacy risks on disclosure (Acquisti 2004; Hoffmann et al. 2016; Spiekermann et al. 2001).

Therefore, we include resignation into the privacy calculus and pose the research question:

In how far influences resignation the effects of benefits and privacy risks on disclosure?

To answer the research question, we rely on the privacy calculus as our basic theory and extend it with research on resignation of individuals. Our study is conducted in the context of social networking sites (SNS). On SNS, much personal information about individuals is disclosed. In many cases, individuals also share information about other individuals giving them less chance to protect their privacy (Biczók and Chia 2013). Also, organizations behind SNS automatically gather information about individuals even without their consent, again, giving them less chance to protect their privacy (Gijzemijter 2015). Consequently, many individuals have also resigned to protect their privacy in the context of SNS (Miller 2017). In this study, we then investigate the consequences of this resignation.

To show what current research has done on that topic we firstly provide information on the privacy calculus and resignation in section two. We then develop our research model in section three, which will be evaluated through an online-based quantitative study. We thereby rely on a sample of 166 participants who were recruited on Amazon Mechanical Turk. The methodology is described in section four. The results of our study are presented in section five, followed by a discussion of the results in section six. Thereby, we show implications of our results for theory and practice. In particular, we contribute by 1) contextualizing resignation in a privacy-related domain, 2) showing that resignation is a concept that can be included into the privacy calculus to better understand the effects of benefits and privacy risks, 3) better explaining the outcome variable which is intention to disclose and 4) explaining that to reduce intention to disclose one needs to reduce the level of resignation.

2 Theoretical background

In this section, we provide a theoretical background on four topics: First, as previous research has indicated that applying the privacy calculus can lead to unexpected results, we explain the basic concepts of the privacy calculus. Second, we show what previous research has done to better explain such unexpected results of the privacy calculus. Based on these sections we carve out the research gap. With this we show that resignation is a concept that has not been considered before to explain disclosure when benefits are low and privacy risks are high. Consequently, we give information on resignation from a psychological point of view and then conceptualize it in the context of privacy.

2.1 Privacy Calculus

Privacy is defined as having the control over ones' personal information (Bélanger and Crossler 2011). Disclosing information leads to potentially losing control whereas disclosure is defined as revealing personal information to another party (Wakefield 2013). Vice versa, protection of privacy is the refusal of information, i.e. the non-disclosure (Son and Kim 2008). The intention to disclose or to refuse

information is based on the privacy calculus, one of the most used theories in privacy research (Dinev and Hart 2006; Wirth 2018).

The privacy calculus includes on the one hand benefits of disclosure. They represent all positive outcomes of disclosure (Dinev and Hart 2006). In the context of social networking sites, perceived enjoyment is often used as an equivalent to benefits (Krasnova et al. 2012; Lin and Lu 2011; Wakefield 2013). On the other hand, disclosure of information entails risks to ones' privacy. Generally, risks are defined as the perception of an individual about the probability of a threat and its adverse consequences (Cox 2008). Privacy risks in a SNS context (Krasnova et al. 2012) would then be the perception of an individual about the probability that a threat occurs, e.g. other individuals disclose personal information about him/her (Biczók and Chia 2013) and its adverse consequences, e.g. identity theft (Dinev 2014).

Based on the privacy calculus, individuals perform a weighing of benefits and privacy risks, which are related to the disclosure of information. To express that from a model-driven point of view, benefits have a positive effect and privacy risks have a negative effect on intention to disclose (see Figure 1). If benefits, which relate to positive outcomes are at least as high as privacy risks which relate to negative outcomes, then maximization of positive outcomes is fulfilled, and individuals will disclose information. If benefits do not outweigh privacy risks, then individuals will not disclose information. That is because individuals try to minimize negative and to maximize positive outcomes (van Eerde and Thierry 1996; Vroom 1964). This calculus is done repeatedly every time when individuals form their intention to disclose information.

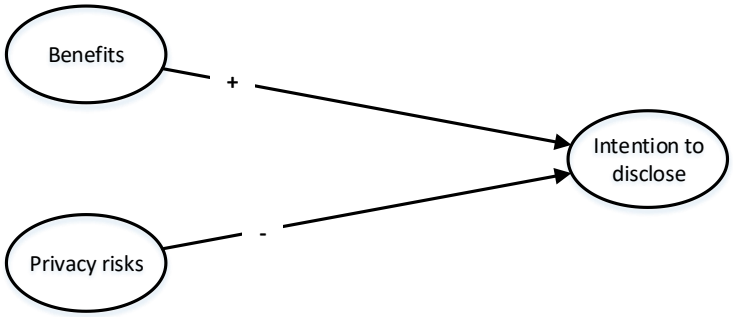

Figure 1. The privacy calculus (Dinev and Hart 2006)

2.2 Further Research to Better Understand the Privacy Calculus

Individuals still disclose information despite only low benefits and high privacy risks which challenges the classic assumption of the privacy calculus (Acquisti 2004). There are two explanations for that issue: 1) Altering the *perception* of benefits and privacy risks and 2) Altering the *effect* of benefits and privacy risks on intention to disclose. Both explanations have different meanings:

1) Altering the *perception*: To alter the perception of benefits and privacy risks, antecedents are used to directly influence both perceptions. Through such antecedents, individuals can have a high perception of benefits although they are actually low and can have a low perception of privacy risks although they are actually high. In such a case, individuals would disclose information because of their perception although from an objective point of view, benefits are low and privacy risks are high. Previous research (i.e. Acquisti 2004) has found out three antecedents altering such perceptions:

The first antecedent is limited information, which means that individuals do not always have access to all necessary information. They evaluate benefits and privacy risks on the basis of such limited amount of information. This can lead to failures in the evaluation process. The second antecedent refers to bounded rationality, which is that even if individuals had access to necessary information, some would not be able to process that information in a sensible way. That means that individuals are not able to calculate and to compare all the consequences associated with disclosure in relation to benefits and privacy risks. The third antecedent is that even if individuals had access to all information and would be

able to calculate all information, they might still have some form of psychological distortion leading to a misperception of benefits and privacy risks (Acquisti 2004).

2) Altering the *effect*: To alter the effect of benefits and privacy risks on intention to disclose moderators are used. A moderator has the potential to alter the strength of the effect of benefits and privacy risks on intention to disclose (Henseler and Fassott 2010). Thereby, the effect of privacy risks can become weak. In such a case, individuals would disclose information despite high privacy risks because the negative effect of privacy risks is rather weak. On the other hand, the effect of benefits can become strong. In such a case, individuals would disclose information despite low benefits because the positive effect of benefits is rather strong.

After having conducted a literature review in the area of privacy in the domain of IS by using search terms such as "privacy calculus", we found four research articles dealing with four moderators, which alter the effect of benefits and privacy risks on intention to disclose. They can be divided into two categories. On the one hand, there are perceptions. In particular, perceived relevance shows that the effect of benefits on intention to disclose becomes weak when the information requested appears to be not relevant. On the other hand, it becomes insignificant when the information seems to be relevant (Sarathy and Li 2007). Perceived trust is another moderator, which alters the effect of benefits on intention to disclose. The effect becomes weak when individuals' level of trust towards the company the information is disclosed to, is high (Xu et al. 2003). Privacy risks has also been shown to moderate the effect of benefits on intention to disclose such that it weakens that effect when privacy risks are high (Sun et al. 2015). On the other hand, besides perceptions, there are mental states, which can also have a moderating influence. Mental states are cognitive conditions at a particular moment in time (Dane 2011). It was shown that when individuals are more in a prevention-focused state, i.e. more focus on losses of disclosure, the effect of benefits on intention to disclose becomes weak whereas the effect of privacy risks on intention to disclose becomes strong (Brakemeier et al. 2016).

2.3 Research gap

Previous research has used perceived relevance (Sarathy and Li 2007), perceived trust (Xu et al. 2003), privacy risks (Sun et al. 2015) and mental states (Brakemeier et al. 2016) as moderators in the privacy calculus. Yet, two research gaps arise: 1) These moderators were used to depict why the effect of benefits was decreased and the effect of privacy risks was increased. However, in this study we aim to find out what moderator decreases the effect of benefits and increases the effect of privacy risks. 2) Previous research has concentrated on perceptions or mental states, yet, leaving out reactions to given events as possible moderators. Reactions have been used as moderators beforehand (Cicchetti 2016; Pirkkalainen et al. 2017) and are therefore used in this study. In particular, we use resignation as a reaction to given events as suggested by previous research (Acquisti 2004; Spiekermann et al. 2001) (see Figure 2).

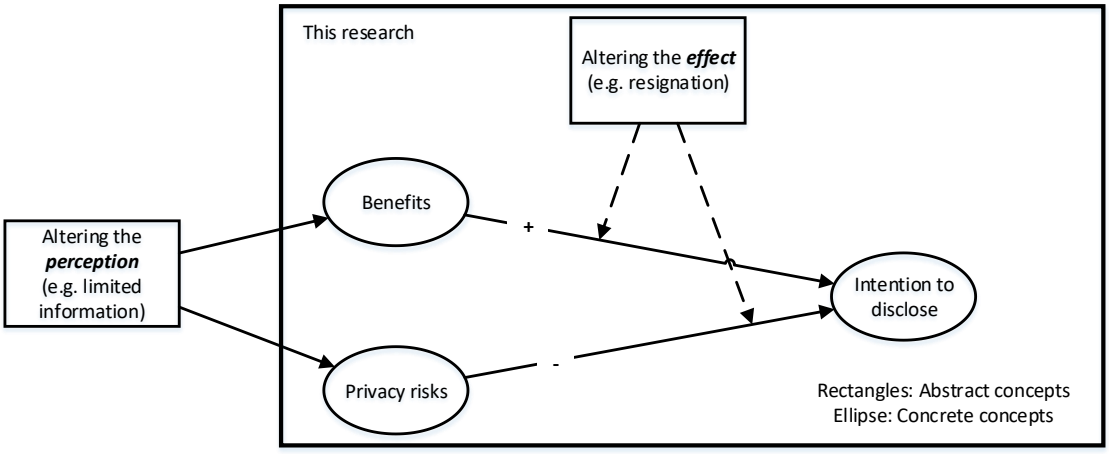

Figure 2. Using resignation as a reaction to alter effects in the privacy calculus

2.4 Resignation to alter the effect

Resignation in psychology: Resignation is a reaction of individuals to given events. Given events are expressed by threats which individuals respond to (Feifel and Strack 1989). A threat is an event that can cause adverse consequences. It therefore needs to be distinguished from risk: Whereas threat is an event that can cause adverse consequences, risk is the perception of an individual about the probability of a threat and its adverse consequences (Cox 2008). Individuals facing a threat evaluate what reaction can be conducted by them to mitigate the threat. If individuals think there is nothing they can do to mitigate the threat, then resignation is a possible reaction (Feifel and Strack 1989). Thereby, individuals try to avoid the threat by hoping that time will take care of the threat and rather passively accept the threat as given (Rotondo et al. 2003). Resignation therefore does not resolve the threat, yet, it helps in managing ones' own feelings to live with the threat by accepting it and by also not undertaking any steps to fight against it.

Resignation is therefore defined as a reaction of individuals that they have to accept a given threat such that they cannot change that threat and therefore also show no signs of changing their situation (Feifel and Strack 1989).

Resignation in the context of privacy: In today`s world there are many privacy-related threats, i.e. events that can cause adverse consequences in relation to ones` privacy. For example, individuals disclose information about other individuals on SNS without asking them (Biczók and Chia 2013). Organizations are gathering personal information about individuals automatically without their consent (Hong and Thong 2013). Governmental agencies are spying on individuals while they are online (Dinev et al. 2008).

Such threats can lead to adverse consequences such as identity theft (Dinev 2014). Exemplary reactions to such threats could be venting, i.e. openly showing emotions (Beaudry and Pinsonneault 2010) or trying to adapt ones´ own behavior (Beaudry and Pinsonneault 2005). Research has shown that in the context of privacy, resignation is another form of reaction individuals can show when facing privacy threats (Hoffmann et al. 2016). These individuals think that privacy protection is futile and that they cannot control their privacy anymore.

Hence, using such research and the definition of resignation from psychology research (Feifel and Strack 1989; Folkman and Lazarus 1980; Lazarus and Folkman 1984), one form of reaction, individuals in the context of privacy can show, is resignation. In particular, the general definition of resignation refers to that individuals accept a given threat, they cannot change that threat and therefore also show no signs of behavior to change their situation (Feifel and Strack 1989). One can use that general definition and adapt it to privacy-related research. We can then define resignation in the context of privacy as an ongoing reaction of individuals that they accept current privacy threats that they cannot protect themselves against these threats and therefore show no signs of behavior to protect their privacy.

3 Research Model

This study aims to find out how resignation is usable to better understand why individuals disclose information despite low benefits and high privacy risks in the context of SNS. To do so our study includes resignation as a moderator into the privacy calculus. Based on the privacy calculus, we include benefits and privacy risks as well as the intention to disclose into our research model (Dinev and Hart 2006). In addition, we include the control variables age and gender as it has been done by related research (Mousavizadeh and Kim 2015). An overview of our research model is given in Figure 3.

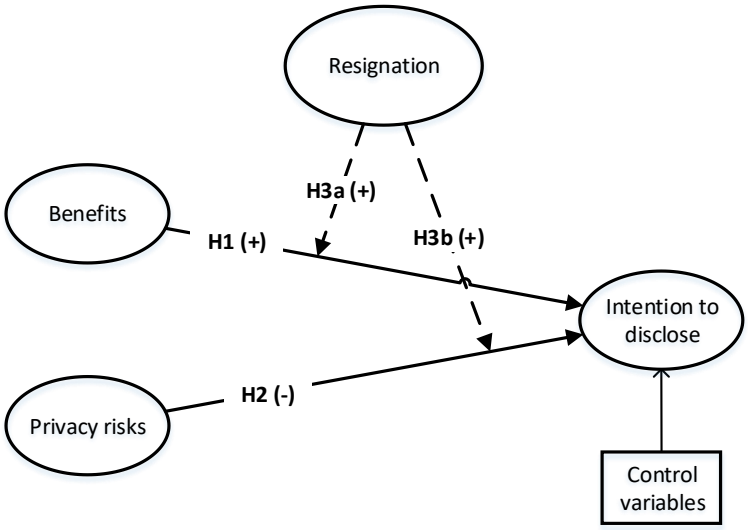

Figure 3. Research model

Disclosure of information can lead to several benefits. For example, monetary incentives (Acquisti and Grossklags 2005) or usefulness (Xu et al. 2012). Individuals try to maximize these benefits (van Eerde and Thierry 1996; Vroom 1964). Therefore, individuals who consider certain benefits to occur when disclosing information increase their intention to disclose information to gain such benefits. This is also the case in the context of SNS, where benefits mainly relate to perceived enjoyment (Lin and Lu 2011) which can be gained when disclosing information (Krasnova and Veltri 2010). In line with previous research (Dinev and Hart 2006), we hypothesize:

H1: The higher the benefits the higher the intention to disclose.

Besides possible benefits, disclosure of information can also lead to several privacy risks. Individuals rate privacy risks as the probability of a threat and its adverse consequences (Cox 2008). Individuals try to avoid these risks to minimize the potential adverse consequences (van Eerde and Thierry 1996; Vroom 1964). As these privacy risks relate to the disclosure of information, individuals, who are facing privacy risks, lower the intention to disclose information to avoid the subsequent privacy risks. Especially on SNS, individuals face several privacy risks such as individuals disclosing information of others resulting in possible identity theft (Dinev 2014). In line with previous research (Dinev and Hart 2006), we hypothesize:

H2: The higher the privacy risks the lower the intention to disclose.

Individuals, who are resigned in protecting their privacy, might still have the same perception of benefits through disclosure than individuals who are not resigned. However, we assume that the effect of benefits on intention to disclose will be different. If individuals are resigned, we assume that they think that there is nothing they can do to protect their privacy due to ongoing privacy threats. Due to these privacy threats individuals think that their information is disclosed anyway. Thus, individuals have two options: Either, they disclose their information on their own and gain the benefits out of disclosure, such as perceived enjoyment. Alternatively, the information is disclosed by someone else, e.g. another individual, but then they will not receive the benefits out of disclosure.

However, individuals try to maximize their positive outcomes (van Eerde and Thierry 1996; Vroom 1964). Disclosure of information by oneself often leads to such positive outcomes (Acquisti 2004; Acquisti and Grossklags 2003; Dinev and Hart 2006). Even if they are very small, we assume that individuals who are resigned will still disclose the information to at least gain these small benefits because these individuals think that information will be disclosed anyway. In other words: We assume that individuals who have resigned in protecting their privacy disclose information when there is even the chance

of the slightest benefits because they think that the information will otherwise be disclosed anyway but without earning the benefits.

For example, on a SNS, an individual who is resigned thinks that either she discloses pictures of last night party with her friends by herself and receives the benefits out of it, such as having fun doing so. Alternatively, a friend who was at the same party is disclosing the pictures, yet, then the friend will earn the benefits out of it. As individuals try to maximize their positive outcomes (van Eerde and Thierry 1996; Vroom 1964) the individual who is resigned will be more likely to consider the benefits when having the intention to disclose. We hypothesize:

> *H3a: Resignation moderates the positive effect of benefits on intention to disclose such that this effect becomes stronger.*

Individuals who have resigned in protecting their privacy can have the same perception of privacy risks than individuals who have not resigned. However, we assume that the effect of privacy risks on intention to disclose will be different. Risks are the probability of a threat and its adverse consequences (Cox 2008). To reduce privacy risks, individuals would try to minimize their exposure to privacy threats. This is done by lowering the amount of information to be disclosed (Dinev and Hart 2006). Yet, we assume that individuals who have resigned in protecting their privacy do not believe that minimizing disclosure will help in mitigating privacy threats. In our research, we hypothesize that these individuals think that no matter what they do, privacy threats will stay omnipresent and will not be reduced when not disclosing information. Therefore, there is no reason to not disclose information due to privacy risks because not disclosing will not help in mitigating threats and therefore also not in mitigating privacy risks.

For example, in a SNS context, individuals face the threat that their information is disclosed without their consent, e.g. by other individuals (Biczók and Chia 2013). This threat can lead to adverse consequences, e.g. identity theft (Dinev 2014). Individuals who are resigned think that not disclosing their information will not reduce privacy threats. They therefore have no reason to not disclose their information on SNS even if privacy risks are high. The effect of privacy risks on intention to disclose should therefore be weaker for individuals who are resigned in protecting their privacy. We hypothesize:

> *H3b: Resignation moderates the negative effect of privacy risk on intention to disclose such that this effect becomes weaker.*

To evaluate our research model, we conducted a quantitative study.

4 Methodology

To evaluate our research model, we conducted a survey. To account for content validity, we used standardized items from previous literature. In particular, for benefits we asked for perceived enjoyment since it is the main benefit when using SNS (Lin and Lu 2011). Our items are adapted from Sun et al. (2015). For privacy risks we use standard items from Malhotra et al. (2004) and for intention to disclose items are adapted from Johnston and Warkentin (2010) as well as Mousavizadeh and Kim (2015) from the privacy-related field. For the items to measure resignation we rely on Feifel and Strack (1989). All items are depicted in Table 3 (see Table 3 in the Appendix). The items were adapted to the context of social networking sites (SNS). The reason is that individuals frequently disclose information on SNS and therefore privacy is especially threatened in such a context. In particular, at the beginning of the survey, we gave participants the information that SNS include Facebook, WhatsApp, Twitter, YouTube or similar. Individuals should then provide answers to our survey items, which included the term 'social networking sites' (SNS).

To conduct the survey, we relied on Amazon Mechanical Turk (mTurk) which is an online crowdsourcing market (OCM). On such an OCM, individuals earn money for participating in surveys. mTurk has been successfully validated by previous research (Steelman et al. 2014) and it is also considered to be equivalent if not superior to other research methods (Lowry et al. 2016). mTurk has also been successfully used in privacy settings (Bellekens et al. 2016; Pu and Grossklags 2015).

In particular, we put the questionnaire online on our own server, using Limesurvey and then put a link on mTurk to ask workers to conduct our survey. We gave respondents a maximum of ten minutes to conduct the survey and paid each participant $0.20. We followed the guidelines of previous research to conduct the survey, e.g., by only letting participants take part who have a high ratio of successful completed tasks. All in all, 180 individuals took part in our survey. Following recommendations of previous research, we also included a trap question (Lowry et al. 2016). Participants who failed to correctly answer on that question were removed. We then ended up with a total of 166 participants. The average age of the participants is 32.21 years with a standard deviation of 10.56 years. 45.2 percent are female, 54.8 percent are male.

We performed a structural equation modeling approach by using SmartPLS 3.2.6 (Hair et al. 2017). The results of the model are presented in the following section.

5 Results

The validation of our research model is done by evaluating the measurement model, followed by an evaluation of the structural model. Before evaluating the measurement model, one should also account for common method bias.

5.1 Common method bias

When checking on common method bias we can evaluate in how far our results are distorted (Schwarz et al. 2017). We used the widely used Harman's Single-Factor Test, which shows that 36.61 percent is explained by one factor which is below the threshold of 50.0 percent. We then also accounted for the unmeasured latent method construct by including a common method factor (Williams et al. 2003). The average R^2 including the common method factor is 80.92 percent and excluding the common method factor is 80.74 percent. Therefore, the common method factor explains a delta of 0.18 which is a ratio of 1:456. These tests therefore show no indication of common method bias in our data (Liang et al. 2007).

5.2 Measurement model

To evaluate the measurement model when using reflective indicators as in our study, one needs to account for indicator reliability, construct reliability and discriminant validity. To evaluate indicator reliability, each indicator should explain more than 50 percent of the variance of the latent variable. Therefore, each value needs to be at least 0.707 (Carmines and Zeller 2008) which is the case in our study (see Table 3 in the appendix). Each loading is also significant with $p<0.001$.

Construct	Mean	SD	AVE	CR	1	2	3	4	5	6
1 Benefits	3.30	1.76	0.900	0.945	**0.949**					
2 Privacy risks	5.33	1.23	0.764	0.907	-0.253	**0.874**				
3 Intention to disclose	3.56	1.70	0.895	0.962	0.623	-0.371	**0.946**			
4 Resignation	4.12	1.52	0.772	0.910	0.252	0.112	0.154	**0.879**		
5 Age	32.21	10.56	n/a	n/a	0.193	-0.175	0.337	-0.011	n/a	
6 Gender	1.45	0.50	n/a	n/a	-0.070	-0.027	-0.045	-0.074	-0.010	n/a

Note: Square root of AVE (bold) is listed on the diagonal of bivariate correlations.

n/a cannot be evaluated because these constructs are single-item constructs

All items were measured on a 7-point Likert scale, ranging from strongly disagree (1) to strongly agree (7)

Table 1. AVE, CR, and bivariate correlations

To account for construct reliability, one needs to assess the average variance extracted (AVE) which should be greater than 0.5 as well as the composite reliability (CR), which should be greater than 0.7 (Fornell and Larcker 1981). Both is the case as depicted in Table 1. Discriminant validity is assessed to

make sure that the constructs differ from each other. To do so, one needs to compute the square root of the AVE and needs to check on in how far this value is greater than the correlation of the constructs with each other (Fornell and Larcker 1981; Hulland 1999). This is also the case in our study (see Table 1). Additionally, we also computed the heterotrait-monotrait ratio (HTMT, Henseler et al. 2014). When using the most conservative approach $HTMT_{0.85}$ we do not observe any lack of discriminant validity, since the highest correlation is between intention to disclose and benefits with 0.660. As all requirements have been fulfilled, we can state that our measurement model is valid.

5.3 Structural model

To evaluate the structural model, we accounted for the variance explained (R^2) as well as for the level of path-significance (Chin 1998). Beforehand, we also accounted for the overall model fit (Henseler et al. 2016). The test of the saturated model shows that standardized root mean square residual is 0.052 and therefore below the recommended value of 0.08 (Hu and Bentler 1999). Therefore, the overall fit of the model is given. The results of the structural model show that all four hypotheses have been supported (see Figure 4).

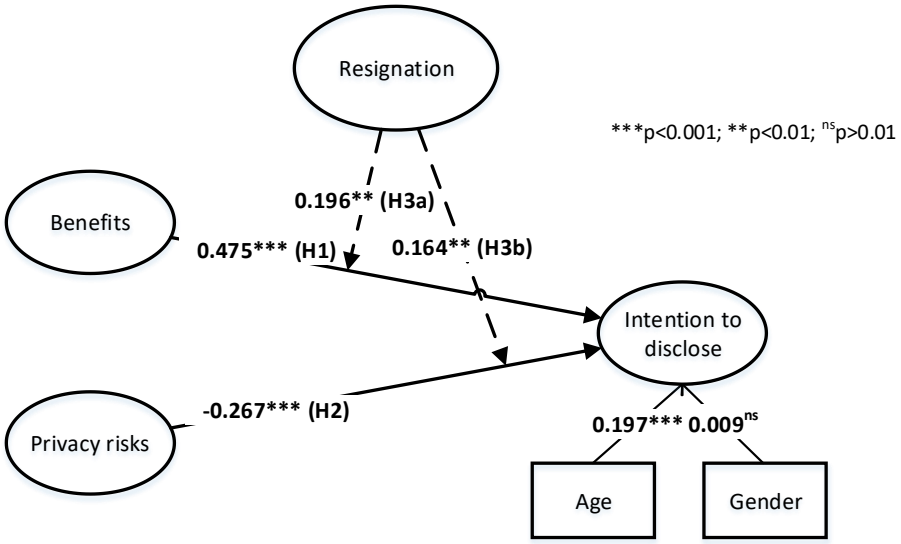

Figure 4. Structural model

In particular, the results show that the intention to disclose is – as predicted by the privacy calculus – dependent on benefits and privacy risks whereas benefits have a positive influence (H1 is supported) and privacy risks have a negative influence (H2 is supported). Besides, we show that resignation positively moderates the effect of benefits on intention to disclose (H3a is supported). That means, that the higher the resignation the stronger the effect of benefits on intention to disclose. We also show that resignation has a positive moderating influence on the effect of privacy risks on intention to disclose (H3b is supported). That means that the negative effect of privacy risks on intention to disclose is weakened by the positive moderating effect of resignation.

When the research model contains a moderator, then one should report the R^2 values of the research model with and without the moderator (Carte and Russell 2003). The explained variance of intention to disclose, expressed by R^2, just using benefits and privacy risks, amounts to 43.7 percent. Including the moderating effect of resignation on the relationship between benefits and intention to disclose (H3a) then R^2 increases to 47.0 percent. Including the moderating effect of resignation on the relationship between privacy risks and intention to disclose (H3b) then R^2 increases to 46.0 percent. Including both moderating effects, R^2 is 50.2 percent. Including the control variables, R^2 is 53.9 percent. Throughout this process, all paths remain significant.

We also calculated the f^2 values as depicted in Table 2. These values show the predictive power of each construct to explain the dependent variable. Thereby, one needs to distinguish between direct

antecedents and moderators because there are different boundaries to evaluate the f^2 value. The results thereby indicate that besides benefits as a strong predictor with a f^2 value of 0.394 (Cohen 1988) also both moderating effects have a strong explanatory power for the dependent variable with f^2 values of 0.098 and 0.060 respectively.

Direct antecedent	**f^2 value**
Benefits	0.394 (strong)
Privacy risks	0.131 (weak)
Age	0.079 (weak)
Gender	0.000 (non-existent)
In general: >0.35 = strong; >0.15 = medium; >0.02 = weak (Cohen 1988)	
Moderators	**f^2 value**
Moderator resignation on benefits	0.098 (strong)
Moderator resignation on privacy risks	0.060 (strong)
Moderator variable: >0.025 = strong; >0.010 = medium; >0.005 = weak (Kenny 2015)	

Table 2. Strength of effect on intention to disclose

5.4 Limitations

Before we discuss the results of our study, we show the limitations of this work. First, previous research is not clearly distinguishing between threats and risks (Pechmann et al. 2003; Rogers and Prentice-Dunn 1997). As resignation is directly determined by threats (Feifel and Strack 1989) and not by risks it seems logical to not relate privacy risks and resignation. Consequently, we also did not find a significant relationship between privacy risks and resignation (see Table 1). Yet, both concepts, risks and threats are still related with each other (Cox 2008). Therefore, future research could further investigate the difference between threats and risks and also check on the relationship with resignation. Second, we used intention to disclose rather than actual disclosure because we rely on the privacy calculus which uses intention to disclose (Dinev and Hart 2006). This rationale has also been used by other studies as well (e.g. Brakemeier et al. 2016). Still, actual disclosure might more contribute to the privacy research stream and therefore future research might research on actual disclosure. Third, previous research states that context matters in privacy-related research (Nissenbaum 2010). We therefore use the context of SNS. Hence, our results are firstly only generalizable to a SNS context, yet, we do not see indications why our results should not be applicable to other contexts, as well. Fourth, based on the definition of resignation (Feifel and Strack 1989) we consider resignation in the privacy context as an enduring reaction which is relatively stable over time. Thus, we consider resignation as a reaction that is already created before individuals conduct the privacy calculus. Still, this is not proven with our study and needs further attention by future research. Fifth, we use particular constructs to measure the privacy calculus. Scholars might also use other constructs, such as perceived usefulness for benefits, to gain additional insights into our research model (Lin and Lu 2011). In addition, controlling for more concepts, such as internet experience, past invasion of privacy or media exposure (Sarathy and Li 2007) might have revealed additional insights into our research model.

6 Discussion

Previous research has proven the privacy calculus, yet, has also challenged it since it was shown that individuals sometimes disclose information despite only low benefits and high privacy risks (Acquisti 2004). There are two explanations for that issue: 1) Altering the *perception* of benefits and privacy risks (Acquisti 2004; Dinev et al. 2015) and 2) Altering the *effect* of benefits and privacy risks on intention to disclose (Brakemeier et al. 2016). Whereas there have been several explanations given for the first one, previous research lacks research on the second explanation. With this research study, we fill that

research gap by providing resignation of individuals as an explanation for that occurrence in the context of SNS.With our study, we therefore contribute to theory in the following ways:

Contextualizing resignation as a reaction to threats in the context of privacy: Resignation has been used in a variety of settings to explain how individuals react to threats in particular situations (Cornelius and Caspi 1987; Feifel and Strack 1989). Yet, to the best of our knowledge, it has not been used in the context of privacy although it can be a common reaction of individuals (Hoffmann et al. 2016). We are therefore the first to use resignation in a privacy-related context. We thereby contextualize and define resignation, based on previous literature, as a reaction of individuals that they have to accept current privacy threats such that they cannot protect themselves against these privacy threats and therefore also show no signs of behavior to protect their privacy. Future research can use this contextualized definition of resignation in privacy-related research contexts (Nissenbaum 2010; Smith et al. 2011).

Proving resignation as a moderator on the effect of benefits and privacy risks on intention to disclose: With our research, we contribute to the research stream that challenges the privacy calculus. Previous research streams have thereby focused on how the perceptions of benefits and privacy risks can be altered, stating several explanations for why benefits and privacy risks might be miscalculated (Acquisti 2004). Previous research has also used several moderators to show how the effect of benefits and privacy risks on disclosure can be altered. Yet, previous research has two research gaps: 1) the used moderators do not explain why individuals disclose information despite low benefits and high privacy risks and 2) resignation as a reaction to events has not been used as a moderator although reactions in general have been proven to be useful moderators (Cicchetti 2016; Pirkkalainen et al. 2017). Therefore, we use resignation as a reaction to certain events and include it in the privacy calculus.

We show that on the one hand, if individuals are resigned the negative effect of privacy risks becomes rather low, i.e. individuals do less decrease their intention to disclose due to privacy risks. This is because these individuals think on a SNS their information will be disclosed anyway, e.g. because of other individuals disclosing their personal information (Biczók and Chia 2013) or organizations gathering their personal information automatically (Gijzemijter 2015). They therefore do not think that they can decrease privacy threats when not disclosing information.

On the other hand, if individuals are resigned, the positive effect of benefits on intention to disclose becomes rather strong, i.e. individuals' intention to disclose is increased due to benefits. This indicates that if individuals are resigned they think their information will be disclosed anyway such that they cannot protect their privacy anymore. They therefore have the choice to either disclose the information by themselves to earn the benefits or to not disclose the information and then also not earn the benefits. As individuals try to maximize their positive outcomes (van Eerde and Thierry 1996; Vroom 1964) even small benefits will lead them to have a higher intention to disclose.

Previous research focusing on antecedents of benefits and privacy risks have furthered our understanding of why individuals disclose information despite low benefits and high privacy risks (Acquisti 2004). The explanations provided relate to incomplete information, bounded rationality and psychological distortions. Yet, even if an individual had access to all necessary information, had all the mental capabilities and had no psychological distortions, our results indicate that in the context of SNS such an individual might still have a high intention to disclose information when she is resigned, even in light of low benefits and high privacy risks. Generally spoken, understanding how perceptions of benefits and privacy risks emerge is important (Acquisti 2004), yet, we contribute by showing that it is also important to understand the effect of these perceptions on intention to disclose.

Explaining intention to disclose by using resignation as a moderator: Intention to disclose is one of the key variables in privacy research (Smith et al. 2011; Wirth 2018), especially in a SNS context (Krasnova and Veltri 2010). Our results show that when including resignation, one can better explain intention to disclose. Accordingly, f^2 values show that resignation as a moderator is important to explain the dependent variable (Brakemeier et al. 2016; Chin 1998; Kenny 2015).

Therefore, we show that besides explaining why the effect of benefits can become strong and the effect of privacy risks can become weak, using resignation as a moderator also helps in explaining intention to disclose in the context of SNS. Previous research has already proven the importance of moderators in

the domain of technology acceptance research (Sun and Zhang 2006). We contribute to that research stream by showing that moderators also seem to be important in privacy research. As resignation as a moderator even had more power to explain intention to disclose than privacy risks, future research might follow that path and include other moderators which might help in explaining intention to disclose.

Decreasing resignation helps in decreasing disclosure: Individuals in todays' world are facing many privacy threats and at the same time have the temptation to still disclose their information because of the tempting prospect to gain certain benefits out of disclosure. Research has consequently shown that such privacy risks might be underrated, whereas benefits might be overrated (Acquisti and Grossklags 2003). If one wants other individuals to lower their intention to disclose to protect their privacy, such results would recommend, to increase individuals' perception of privacy risks and to decrease individuals' perception of benefits.

This might be correct, yet, our results indicate that even when doing so, individuals' intention to disclose at least on SNS might still hardly be affected when these individuals are resigned. This is because individuals' level of resignation weakens the effect of privacy risks and strengthens the effect of benefits. Based on our results we therefore call for a different approach to decrease individuals' intention to disclose: Rather than decreasing the perception of benefits and privacy risks, one needs to decrease the level of resignation. Based on the definition of resignation in a privacy-related context, resignation is mainly determined by accepting privacy threats and thinking that one cannot protect against privacy threats. Hence, to eliminate resignation, individuals' level of acceptance and perception of not being able to protect against a threat needs to be reduced. For example, individuals should be given help how to protect against privacy threats, e.g. by falsifying information (Son and Kim 2008). They need to be enlightened that individuals do not have to accept privacy threats but have a right for privacy (Warren and Brandeis 1890). Individuals should be given technical measures to show how to use social networking sites (SNS) such that information is not used by others. Furthermore, individuals should be enlightened that they also need to protect the privacy of other individuals around them, especially on SNS (Biczók and Chia 2013). Such measures could help to reduce the level of acceptance of privacy threats and to increase the grasp of how to protect against privacy threats.

7 Conclusion and Future Research

Previous research has shown that individuals disclose information despite low benefits and high privacy risks and has focused on antecedents of perceptions of benefits and privacy risks. This study is using a different approach and is considering the effect of benefits and privacy risks on disclosure. The results indicate that the higher the resignation the stronger/the weaker the effect of benefits/privacy risks on intention to disclose. Implications are among others that changing ones' perception of benefits and privacy risks might not be enough to alter the intention to disclose, yet, one needs to change the level of resignation.

Based on our results we also suggest three possibilities for future research. First, we know from previous research that there is also a privacy paradox which is that privacy concerns hardly affect intention to disclose (Kokolakis 2015). Future research could use resignation again as a moderator to find out in how far it might reveal additional insights into the privacy paradox. Second, we recommend changing individuals' level of resignation to have an effect on subsequent disclosure. To change resignation, one needs to understand what leads to resignation. In this research we have considered the outcomes of resignation, future research could thusly focus on the antecedents of resignation which is generally essential to better understand a research model (Wirth et al. 2017). Third, future research could also draw on creating a concept reflecting a fit between benefits and privacy risks. Using the current privacy calculus, benefits and privacy risks are treated as independent concepts, yet, they might be related in some way (Sun et al. 2015). Future research could therefore on the one hand try to find out if there is a concept, which depicts benefits and privacy risks on a continuum. On the other hand, scholars could research on resignation altering the effect of that newly created concept on intention to disclose.

8 Appendix

Construct	Items	Loading	Author(s)
Benefits	I find disclosing my personal information on social networking sites to be enjoyable.	0.947	Sun et al. 2015
	The actual process of disclosing my personal information on social networking sites is pleasant.	0.953	
	I have fun disclosing my personal information on social networking sites.	0.947	
Privacy risks	In general, it would be risky to disclose my personal information on social networking sites.	0.827	Malhotra et al. 2004
	There would be high potential for loss associated with disclosing my personal information on social networking sites.	0.881	
	There would be too much uncertainty associated with giving my personal information on social networking sites.	0.913	
Intention to disclose	I intend to disclose my personal information on a social networking site in the future.	0.958	Johnston and Warkentin 2010; Mousavizadeh and Kim 2015
	I anticipate that I will reveal my personal information on a social networking site in the future.	0.928	
	I plan to disclose my personal information on a social networking site in the future.	0.951	
Resignation	I realize that there is nothing I can do about to actually protect my personal information on social networking sites.	0.865	Feifel and Strack 1989
	I feel that actually protecting my personal information on social networking sites is beyond my control.	0.824	
	I feel that whatever I would do to protect my personal information on social networking sites would not matter.	0.942	
All items were measured on a 7-point Likert scale, ranging from strongly disagree (1) to strongly agree (7)			

Table 3. Items

9 References

Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *Proceedings of the 5th ACM conference on Electronic commerce*, New York, NY, USA: ACM, pp. 21–29.

Acquisti, A., and Grossklags, J. 2003. "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," *2nd Annual Workshop on "Economics and Information Security"* (UC Berkeley).

Acquisti, A., and Grossklags, J. 2005. "Uncertainty, Ambiguity and Privacy," *WEIS* .

Beaudry, A., and Pinsonneault, A. 2005. "Understanding User Responses to Information Technology: A Coping Model of User Adaptation," *MIS Quarterly* (29:3), pp. 493–524.

Beaudry, A., and Pinsonneault, A. 2010. "The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use," *MIS Quarterly* (34:4), p. 689.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.

Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., and Seeam, A. 2016. "Pervasive eHealth services a security and privacy risk awareness survey," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, London, United Kingdom, IEEE, pp. 1–4.

Biczók, G., and Chia, P. H. 2013. "Interdependent Privacy: Let Me Share Your Data," in *Financial cryptography and data security*, A.-R. Sadeghi (ed.), Berlin: Springer, pp. 338–353.

Boyd, D. M., and Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), pp. 210–230.

Brakemeier, H., Widjaja, T., and Peter Buxmann 2016. "Calculating with different goals in mind - The moderating role of the regulatory focus in the privacy calculus," *Research Papers* .

Carmines, E. G., and Zeller, R. A. 2008. *Reliability and validity assessment*, Newbury Park, California: Sage Publications.

Carte, T. A., and Russell, C. J. 2003. "In Pursuit of Moderation: Nine Common Errors and Their Solutions," *MIS Quarterly* (27:3), pp. 479–501.

Chin, W. W. 1998. "The partial least squares approach to structural equation modeling," in *Modern methods for Business Research*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295–336.

Cicchetti, D. (ed.) 2016. *Theory and method*, Hoboken, New Jersey: Wiley.

Cohen, J. 1988. *Statistical power analysis for the behavioral sciences*, Hillsdale, N.J.: L. Erlbaum Associates.

Cornelius, S. W., and Caspi, A. 1987. "Everyday problem solving in adulthood and old age," *Psychology and Aging* (2:2), pp. 144–153.

Cox, L. A. T. 2008. "Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks," *Risk analysis : an official publication of the Society for Risk Analysis* (28:6), pp. 1749–1761.

Dane, E. 2011. "Paying Attention to Mindfulness and Its Effects on Task Performance in the Workplace," *Journal of Management* (37:4), pp. 997–1018.

Dinev, T. 2014. "Why would we care about privacy?" *European Journal of Information Systems* (23:2), pp. 97–102.

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

Dinev, T., Hart, P., and Mullen, M. R. 2008. "Internet privacy concerns and beliefs about government surveillance – An empirical investigation," *The Journal of Strategic Information Systems* (17:3), pp. 214–233.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* , pp. 636–655.

Feifel, H., and Strack, S. 1989. "Coping with conflict situations: Middle-aged and elderly men," *Psychology and Aging* (4:1), pp. 26–33.

Folkman, S., and Lazarus, R. S. 1980. "An Analysis of Coping in a Middle-Aged Community Sample," *Journal of Health and Social Behavior* (21:3), pp. 219–239.

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

Gijzemijter, M. 2015. *Facebook is gathering personal information without consent,' says Belgian privacy watchdog*. http://www.zdnet.com/article/facebook-is-gathering-personal-information-without-consent-belgian-privacy-watchdog/. Accessed 14 November 2017.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: Sage.

Henseler, J., and Fassott, G. 2010. "Testing Moderating Effects in PLS Path Models: An Illustration of Available Procedures," in *Handbook of Partial Least Squares: Concepts, Methods and Applications*, V. Esposito Vinzi, W. W. Chin, J. Henseler and H. Wang (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 713–735.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2014. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 1–21.

Hoffmann, C. P., Lutz, C., and Ranzini, G. 2016. "Privacy cynicism: A new approach to the privacy paradox," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (10:4).

Hong, W., and Thong, J. 2013. "Internet privacy concerns: An integrated conceptualization and four empirical studies," *MIS Quarterly* (37:1), pp. 275–298.

Hulland, J. 1999. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies," *Strategic Management Journal* (20:2), pp. 195–204.

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), 549-A4.

Kenny, D. A. 2015. *Moderator Variables*. http://www.davidakenny.net/cm/moderation.htm. Accessed 27 October 2015.

Kokolakis, S. 2015. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* , pp. 122–134.

Krasnova, H., and Veltri, N. F. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in *43rd Hawaii International Conference on System Sciences (2010)*, R. Sprague and S. Laney (eds.), Koloa, Kauai, Hawaii, pp. 1–10.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127–135.

Lazarus, R. S., and Folkman, S. 1984. *Stress, appraisal, and coping*, New York: Springer.

Lee, R., and Maeve, D. 2016. *Privacy and Information Sharing*. http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/. Accessed 9 October 2017.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS Quarterly* (31:1), pp. 59–87.

Lin, K.-Y., and Lu, H.-P. 2011. "Why people use social networking sites: An empirical study integrating network externalities and motivation theory: Group Awareness in CSCL Environments," *Computers in Human Behavior* (27:3), pp. 1152–1161.

Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. ""Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels," *The Journal of Strategic Information Systems* (25:3), pp. 232–240.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model: Information Systems Research," *Information Systems Research* (15:4), pp. 336–355.

Miller, J. 2017. *How Facebook's tentacles reach further than you think*. http://www.bbc.com/news/business-39947942. Accessed 13 November 2017.

Morgan, J. 2014. *Privacy Is Completely And Utterly Dead, And We Killed It*. https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#3345e1c331a7. Accessed 9 October 2017.

Mousavizadeh, M., and Kim, D. J. 2015. "A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.

Nissenbaum, H. F. 2010. *Privacy in context*: *Technology, policy, and the integrity of social life*, Stanford, California: Stanford Law Books an imprit of Standford University Press.

Ortiz de Guinea, A., and Webster, J. 2013. "An Investigation of Information Systems Use Patterns: Technological Events as Triggers, the Effect of Time, and Consequences for Performance," *Management Information Systems Quarterly* (37:4), pp. 1165–1188.

Pechmann, C., Zhao, G., Goldberg, M. E., and Reibling, E. T. 2003. "What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes," *Journal of marketing* (67:2), pp. 1–18.

Pirkkalainen, H., Salo, M., Makkonen, M., and Tarafdar, M. 2017. "Coping with Technostress: When Emotional Responses Fail," in *Thirty Eighth International Conference on Information Systems*, South Korea.

Pu, Y., and Grossklags, J. 2015. "Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.

Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection motivation theory," in *Handbook of health behavior research 1: Personal and social determinants*, New York, NY, US: Plenum Press, pp. 113–132.

Rotondo, D. M., Carlson, D. S., and Kincaid, J. F. 2003. "Coping with multiple dimensions of work-family conflict," *Personnel Review* (32:3), pp. 275–296.

Sarathy, R., and Li, H. 2007. "Understanding Online Information Disclosure As a Privacy Calculus Adjusted by Exchange Fairness," in *Twenty Eighth International Conference on Information Systems*, B. Gallupe and A. Pinsonneault (eds.), Montreal, Quebec, Canada.

Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldan, J. L., and Barrera-Barrera, R. 2017. "Examining the Impact and Detection of the "Urban Legend" of Common Method Bias," *ACM Sigmis Database* (48:1), pp. 93–119.

Smith, J. H., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 980–1015.

Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503–529.

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior," *Proceedings of the 3rd ACM conference on Electronic Commerce* , pp. 38–47.

Steelman, Z. R., Hammer, B. I., and Limayem, M. 2014. "Data Collection in the Digital Age: Innovative Alternatives to Student Samples," *MIS Quarterly* (38:2), pp. 355–378.

Sun, H., and Zhang, P. 2006. "The role of moderating factors in user technology acceptance," *HCI research in privacy and security* (64:2), pp. 53–78.

Sun, Y., Wang, N., Shen, X.-L., and Zhang, J. X. 2015. "Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences," *Computers in Human Behavior* (52), pp. 278–292.

van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81:5), pp. 575–586.

Vroom, V. H. 1964. *Work and motivation*, New York: Wiley.

Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157–174.

Warren, S. D., and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), pp. 193–220.

Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6), pp. 903–936.

Wirth, J. 2018. "Dependent Variables in the Privacy-Related Field: A Descriptive Literature Review," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3658–3667.

Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2017. "Understanding Privacy Threat Appraisal and Coping Appraisal through Mindfulness," in *Thirty Eighth International Conference on Information Systems*, South Korea, pp. 1–11.

Xu, C., Ryan, S., Prybutok, V., and Wen, C. 2012. "It is not for fun: An examination of social network site usage," *Information & Management* (49:5), pp. 210–217.

Xu, Y., Tan, B., and Hui, K.-L. 2003. "Consumer Trust and Online Information Privacy," in *Twenty-Fourth International Conference on Information Systems*, J. Valacich and L. Jessup (eds.), Seattle, Washington.