COMPUTERS & SECURITY 77 (2018) 226–261

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior

Nina Gerber[a,*], *Paul Gerber*[b], *Melanie Volkamer*[c]

[a] SECUSO, Department of Computer Sciences, Technische Universität Darmstadt, Darmstadt, Germany
[b] Department of Human Sciences, Technische Universität Darmstadt, Darmstadt, Germany
[c] SECUSO, AIFB, Karlsruhe Institute of Technology, Karlsruhe, Germany

ARTICLE INFO

Article history:
Received 6 October 2017
Revised 28 February 2018
Accepted 2 April 2018
Available online 9 April 2018

Keywords:
Privacy paradox
Information privacy
User psychology
Predictor variables
Literature review

ABSTRACT

Although survey results show that the privacy of their personal data is an important issue for online users worldwide, most users rarely make an effort to protect this data actively and often even give it away voluntarily. Privacy researchers have made several attempts to explain this dichotomy between privacy attitude and behavior, usually referred to as 'privacy paradox'. While they proposed different theoretical explanations for the privacy paradox, as well as empirical study results concerning the relationship of individual factors on privacy behavior and attitude, no comprehensive explanation for the privacy paradox has been found so far. We aim to shed light on the privacy paradox phenomenon by summarizing the most popular theoretical privacy paradox explanations and identifying the factors that are most relevant for the prediction of privacy attitude and behavior. Since many studies focus on the behavioral intention instead of the actual behavior, we decided to consider this topic as well. Based on a literature review, we identify all factors that significantly predict one of the three privacy aspects and report the corresponding standardized effect sizes (β). The results provide strong evidence for the theoretical explanation approach called 'privacy calculus', with possibly gained benefits being among the best predictors for disclosing intention as well as actual disclosure. Other strong predictors for privacy behavior are privacy intention, willingness to disclose, privacy concerns and privacy attitude. Demographic variables play a minor role, only gender was found to weakly predict privacy behavior. Privacy attitude was best predicted by internal variables like trust towards the website, privacy concerns or computer anxiety. Despite the multiplicity of survey studies dealing with user privacy, it is not easy to draw overall conclusions, because authors often refer to slightly different constructs. We suggest the privacy research community to agree on a shared definition of the different privacy constructs to allow for conclusions beyond individual samples and study designs.

* Corresponding author.
E-mail addresses: nina.gerber@secuso.org (N. Gerber), gerber@psychologie.tu-darmstadt.de (P. Gerber), melanie.volkamer@kit.edu (M. Volkamer).
https://doi.org/10.1016/j.cose.2018.04.002
0167-4048/

1. Introduction

A multiplicity of digital technologies is used by most individuals in industrialized countries nowadays. These newly obtained technical capabilities certainly offer many benefits, but they also come along with the omnipresence of data capturing devices. Thus, it is not surprising the privacy of their personal data is a major concern for most online users. According to recent survey results, an overwhelming majority of American adults (91%) think that consumers have lost control over how personal information is collected and used by companies (Pew Research Center, 2014) and half of the American internet users worry about the amount of information available about them online (Pew Research Center, 2013). Regarding European users, 57% are worried their personal data is not safe (Symantec, 2015). If we also consider the increase of online privacy concerns between 2013 and 2014 among Asian users (e.g., India, South Korea, Hong Kong, China, Japan), African users (e.g., Nigeria, Egypt, Kenya), South American users (e.g., Brazil), Australian users, and Canadian users (Ipsos and Centre for International Governance Innovation, 2014; Ipsos MORI, 2014), the privacy of personal data seem to be an important issue for users worldwide. The expressed attitudes, however, stand in harsh contrast to the fact that only one in four European users read the terms and conditions in full when buying or signing up to products and services online. Beyond that, 59% confessed to merely skim the terms and conditions when making a purchase, whereas 14% never read them at all. Thirty percent of the respondents would even trade their e-mail address for money or the chance to win a prize or be entered in a raffle and 17% are willing to give it away in exchange for access to an app (Symantec, 2015). Worldwide, 39% report to enforce high privacy settings on social networks, 34% turn off location tracking in apps and only 18% try to avoid using popular data-gathering websites like Google and Facebook (B2B International with Kaspersky Lab, 2015).

Yet this seemingly paradoxical behavior is not a new phenomenon in the privacy research area. For at least ten years now, privacy researchers attempt to explain the so-called 'privacy paradox', which describes the dichotomy of information privacy attitude and actual information privacy behavior (e.g., Acquisti and Grossklags, 2005; Boyd and Ellison, 2007; Norberg et al., 2007; Smith et al., 2011). On the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their e-mail communication.

Privacy researchers have made several attempts to explain the privacy paradox during the last ten years (Kokolakis, 2017). They proposed different theoretical explanations for the privacy paradox, as well as empirical results from various studies dealing with privacy attitude and/or privacy behavior. Nevertheless, no comprehensive explanation has been found so far and user privacy remains a rather complex phenomenon that cannot entirely be explained yet (Kokolakis, 2017). The present paper therefore aims to shed light on the privacy paradox by summarizing the most popular theoretical privacy paradox explanations and taking a closer look at the factors that have been shown to significantly relate to user privacy. Based on a literature review for the search term 'privacy paradox', we tried to identify all factors that significantly predict privacy attitude and privacy behavior. Therefore, we first collected all articles that contain study results from either regression analyses or structural equation models dealing with the relationship of various predictor variables with at least one of the two privacy aspects. Although privacy attitude originally refers to the general appraisal of different privacy behaviors, it is often operationalized as the assessment of privacy concerns or perceived risk, respectively. We will therefore consider all three approaches. Since many studies focus on the behavioral intention instead of the actual behavior, we decided to include this topic as well. We report the standardized effect size (β) that could be found in the included studies concerning the association of the different predictor variables with one of the privacy concepts.

The remainder of this paper is organized as follows: In section two, the methodological procedure is described, section three summarizes the most popular theoretical explanation attempts for the privacy paradox, section four focusses on the empirical explanation attempts for the privacy paradox (i.e., the standardized effect sizes for all identified predictor variables are reported) and section five provides a detailed discussion of the results, including the implications the empirical study results hold for the theoretical privacy paradox explanation attempts.

2. Method

We first conducted a literature search, resulting in a primary list of 181 articles dealing with the privacy paradox. Based on these articles, we identified the most popular theoretical explanation attempts for the privacy paradox. To identify the factors that are most appropriate for the prediction of privacy attitude, concerns, perceived risk, behavioral intention and behavior, we then excluded all articles that (a) provide empirical evidence only based on the opinion of experts, (b) do not describe quantitative user studies and (c) do not contain study results from regression analyses or structural equation modeling dealing with the relationship of various variables with at least one of the above mentioned privacy aspects. We further rated the quality of the included studies, but did not exclude any article or study based on its quality rating. The methodological procedure is displayed in Fig. 1.

2.1. *Literature search*

We used the keyword 'privacy paradox' to search for publications dealing with this topic in the databases Google Scholar, ACM Digital Library, IEEE Xplore Digital Library and Scopus. The search process took place between November 2015 and February 2016. We excluded papers which were not published in English or before 2006, since technological solutions affect-

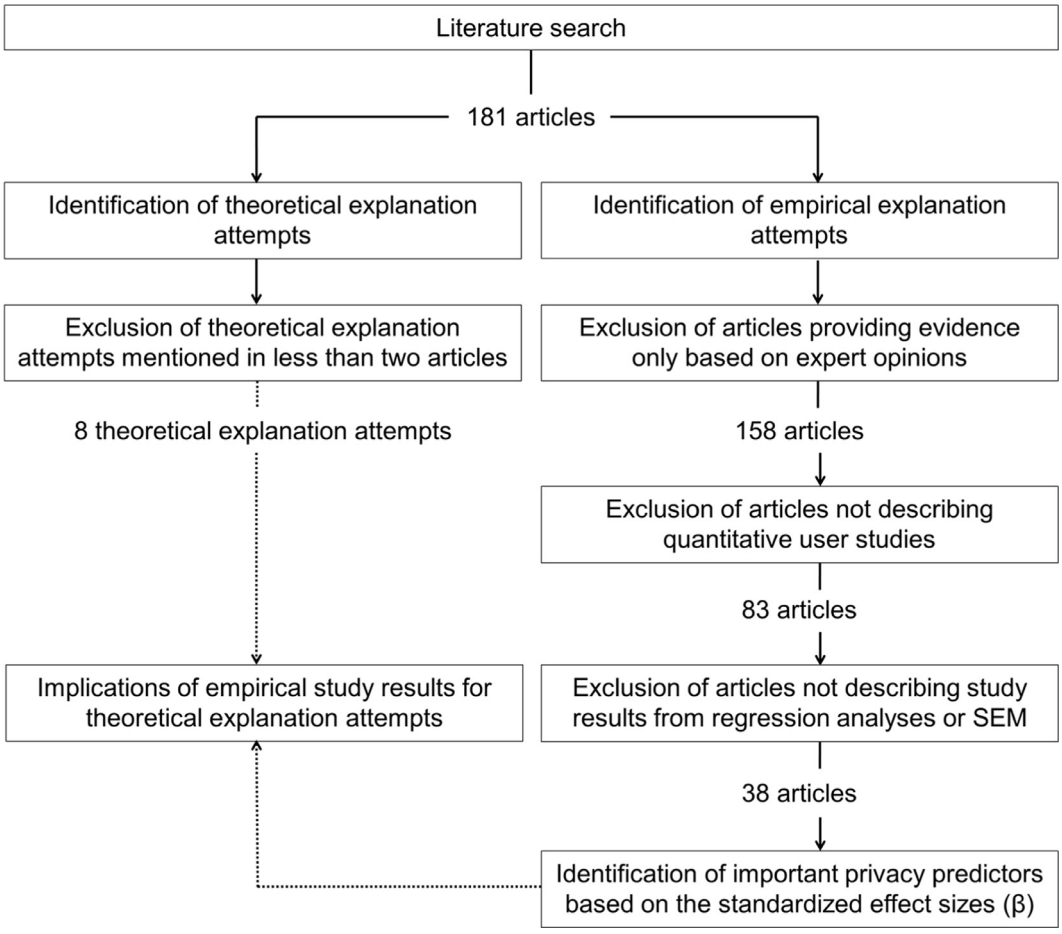


Fig. 1 – Graphical depiction of the review procedure.

ing privacy in the daily life of users like Smartphones or the Internet of Things have been evolving rapidly in the last ten years. Therefore, empirical results that are obtained before 2006 may be based on different understandings of digital privacy and, as a consequence, differ systematically from newer findings.

Our preliminary list included 181 articles dealing with the privacy paradox. We identified eight theoretical explanation attempts for the privacy paradox which were referred to in at least two articles. These are summarized in section three. Of the 181 included articles, 53 dealt with the privacy behavior of users (41 assessed data disclosure behavior, 30 data protection behavior). The behavioral intention was examined in 39 articles, whereas privacy attitude was assessed in 12, privacy concerns in 47 and perceived privacy risk in 20 articles.

2.2. *Inclusion of study results*

We decided about the inclusion of study results in the further evaluation based on the guidelines for performing a systematic literature review in the area of software engineering by Kitchenham (2004). She distinguishes between five different levels of evidence drawn from empirical studies, based on the particular study design: Level 1 includes randomized controlled trials and level 2 pseudo-randomized controlled trails (i.e., the allocation to the treatment is not random) and level 5 the assessment of expert opinions based on theory or consensus. No study design can definitely be assigned to level 3 and 4, however, there are several study designs that can be assigned to more than one level, namely randomized experiments that are performed in an artificial setting (level 1–4), comparative studies with non-randomized concurrent controls and allocation, cohort studies, case-control studies or interrupted time series with a control group (level 1–3), comparative studies with historical control, two or more single arm studies, or interrupted time series without a parallel control group (level 2–3), post-test or pre-test/post-test case series (level 2–4) and quasi-randomized experiments that are performed in an artificial setting (level 3–4). We included only studies offering evidence on level 1 to 4, i.e., studies which results are based on the opinion of experts were excluded. This is in line with the suggested procedure by Kitchenham (2004) to accept all levels of evidence, except for level 5, which can be excluded if there are a reasonable number of studies that can be assigned to level 1–4. A total of 23 articles were excluded in this step, leaving 158 articles.

Of these 158 articles, 83 contained results from quantitative user studies. The other 75 articles, describing qualitative studies (e.g., semi-structured or unstructured interviews) or studies in which no data from users was assessed (e.g., mere mathematical evaluations of technical solutions), were also excluded.

Thirty-eight of the remaining 83 articles contained study results from either regression analyses or structural equation models dealing with the relationship of various variables with at least one of the above mentioned privacy aspects: attitude, concerns, perceived risk, behavior and behavioral intention. These 38 articles constitute the final set of articles included in the present review. A majority of the included studies (31) is published in journals; however, six of the studies are published in conference proceedings.

2.3. *Quality assessment*

We assessed the methodological quality of the included studies according to the quality attributes for survey research proposed by Malhotra and Grover (1998), as except for one, all of the included studies rely on questionnaire-based surveys. The fourth criterion (Is any form of triangulation used to cross validate results?) was considered as irrelevant for survey studies and therefore excluded. We evaluated the fulfillment of the quality criterions based on the original definitions and on the further detailing developed by Sommestad et al. (2014). Each study was rated independently by three reviewers. Differences in the rating were solved afterwards through group discussion. Although we did not exclude any study on the basis of its quality rating, the reader is invited to evaluate the presented results with respect to the according study quality. The results of the quality assessment and the quality criterions can both be found in the appendix.

We also conducted power analyses for the included studies, using G*Power (Faul et al., 2009) for the regression and the PLS-based SEM analyses and *Free Statistics Calculators* (Soper, 2018) for the covariance-based SEM analyses. Since none of the included studies fails to achieve sufficient power ($\geq .8$), we did not exclude studies based on their lack of statistical power.

The results are presented in the next two sections, starting with a summary of the eight most popular privacy explanation attempts (Section 3), followed by the empirical study results concerning the relationship of different predictor variables and privacy attitude, privacy concern, perceived privacy risk, privacy intention and privacy behavior (Section 4).

3. Theoretical privacy paradox explanation attempts

The following section describes the most popular explanations for the privacy paradox that have been proposed so far. A prior review of possible explanation approaches can be found in Kokolakis (2017).

3.1. *Privacy calculus*

One of the most-established explanations for the privacy paradox is based on the theoretical concept of the 'homo oeconomicus'. In the economic sciences, the term 'homo oeconomicus' refers to the prototype of an economic human, a consumer whose decisions and actions are all driven by the attempt to maximize his/her benefits (Rittenberg and Trigarthen, 2012; Flender and Müller, 2012). If this concept is applied to the privacy context, a user is expected to trade the benefits that could be earned by data disclosure off against the costs that could arise from revealing his/her data (Lee and Kwon, 2015). Typical benefits of sharing personal data include financial discounts (e.g., by participating in consumer loyalty programs), increased convenience (e.g., by keeping credit card data stored with an online retailer) or improvement of socialization (e.g., by using social networks and messengers) (Wang et al., 2015; Wilson and Valacich, 2012). Data sharing costs, on the other hand, are less tangible and include all sorts of risk and negative consequences for disclosing personal data (e.g., security impairments, identity theft, unintended third-party usage, or social criticism and humiliation) (Warshaw et al., 2015). According to the privacy calculus model, if the anticipated benefits of data sharing exceed the costs, a user is expected to willingly give his/her data away (Lee and Kwon, 2015). Nevertheless, s/he can still express concerns about the loss of his/her data, leading to the observed discrepancy between the expressed concerns or attitude and the actual behavior.

3.2. *Bounded rationality & decision biases*

The recently described privacy calculus model postulates the existence of a rational user, who performs reasoned trade-off analyses for the decision to share (or protect) his/her data. However, numerous studies on consumer decision behavior have shown that the decision making process is affected by various cognitive biases and heuristics (Acquisti and Grossklags, 2007; Knijnenburg et al., 2013). For example, it is unlikely that every consumer accesses exhaustive information concerning all possible costs and benefits when making a data sharing decision (on the contrary, consumers are often not even aware that their data is being collected (Wakefield, 2013)). Hence, their decision is based on *incomplete information*, which can lead to the over- or underestimation of the costs and benefits and might therefore seem irrational to an external observer, but at the same time fairly rational to the decision maker (Flender and Müller, 2012). Furthermore, the human ability for cognitive processing is limited to a certain degree, which means even if a consumer has access to all necessary information, s/he might lack the ability to process all this information correctly and make an informed decision (Deuker, 2011). In the literature, this effect is often referred to as *bounded rationality* (Flender and Müller, 2012; Knijnenburg et al., 2013). The resulting imperfect decisions often suffer from cognitive biases, because the decision maker employs certain heuristics to compensate for his/her bounded rationality (Kokolakis, 2017; Symantec 2015; Wakefield, 2013; Zafeiropoulou et al., 2013; Tversky and Kahneman, 1974). Hence, the resulting behavior might not reflect the original intention or the expressed attitude towards that behavior. Popular examples for these cognitive biases are:

- The *availability bias:* People tend to overestimate the probability of events they can easily recall, e.g., because they are very present in the media (Schwarz et al., 1991).
- The *optimism bias:* People tend to believe that they are at less risk of experiencing a negative privacy event compared to others (Cho et al., 2010).

- The *confirmation bias:* People tend to search for or interpret information in a way that confirms their beliefs and assumptions (Plous, 1993).
- The *affect bias:* People judge quickly based on their affective impressions, thereby underestimating the risks of things they like and overestimating the risks of things they dislike (Slovic et al., 2002).
- The *immediate gratification bias*, sometimes also referred to as *hyperbolic discounting*: People tend to value present benefits or risks more than those that lie in the future (Acquisti and Grossklags, 2003).
- The *valence effect*: People tend to overestimate the likelihood of favorable events (Gold and Brown, 2009).
- The *framing effect*: People respond differently dependent on the way a question is framed or information is presented (Tversky and Kahneman, 1981).
- The phenomenon of *rational ignorance*: People ignore the potential costs of data sharing because the costs for learning them, e.g., by reading the privacy policies, would be higher than the expected benefits from sharing the data (Downs, 1957).

3.3. *Lack of personal experience and protection knowledge*

Another explanation accounts for the fact that few users have actually suffered from online privacy invasions. As a consequence, most privacy attitudes are based on heuristics or secondhand experiences. However, only personal experiences can form an attitude that is stable enough to significantly influence the corresponding behavior (Dienlin and Trepte, 2015). In addition to the resulting weak association between attitude and behavior, some users might simply lack the ability to protect their data, because they have no or only limited knowledge of technical solutions like the deletion of cookies, the encryption of e-mails or the anonymization of communication data, e.g., by using the Tor software (Baek, 2014).

3.4. *Social influence*

Most people are not autonomous in their decision to accept or reject the usage of a messaging application, a social network or e-mail encryption software, respectively. It is rather assumed that the social environment of an individual significantly influences his/her privacy decisions and behavior (Taddicken, 2014). Especially in collectivistic cultures, where individuals possess a strong 'we' consciousness, do users obey to social norms (Beldad and Citra Kusumadewi, 2015). But social influence does also occur in individualistic cultures, for instance when teenagers align to the example of their parents when it comes to data sharing in social networks (Van Gool et al., 2015). In both kinds of culture include individuals usually at least to some extend the (supposed) opinion and behavior of their peers and/or family in their decision to use a specific technology or reveal their data. If significant others tend to self-disclose personal information, e.g., on social networks, some kind of social pressure can occur, eventually build on an idea of reciprocity, i.e., 'if they disclose data it would be unfair not to do the same' (Flender and Müller, 2012). Sometimes, the decision not to share personal data can even become a social stigma, for anyone who refuses to disclose his/her habits, actions and attitudes 'must have something terrible to hide' (Hull, 2015). Hence, actual behavior is most likely affected by social factors, whereas the expressed attitude supposedly reflects the unbiased opinion of the respective individual.

3.5. *The risk and trust model*

It is most likely that the perceived risk of data-disclosing, as well as the trustworthiness of the recipient affects the data sharing attitude and behavior of an individual. Some authors explain the privacy paradox by assuming that trust has a direct influence on privacy behavior, whereas the perceived risk influences the reported attitude and behavioral intention. Still this influence is not strong enough to affect the actual behavior (Norberg et al., 2007). Trust, which is an environmental factor, has a stronger effect in concrete decision situations (i.e., behavior). The perceived risk, on the other hand, dominates in abstract decision situations, for example when a user is asked if s/he would be willing to share his/her data in a hypothetical situation (Flender and Müller, 2012), thereby producing the dichotomy between the reported attitude and the actual behavior.

3.6. *Quantum theory*

Relying on quantum theory, Flender and Müller (2012) propose another explanation for the privacy paradox. If human decision-making underlies the same effects as the measurement process in quantum experiments, we can assume that the outcome of a decision process is not determined until the actual decision is made (Kokolakis, 2017) and two decisions are not interchangeable in terms of decision making (Flender and Müller, 2012). Hence, if an individual is asked about a potential decision outcome prior to actually making the decision (i.e., attitude rather than behavior is assessed), his/her answer does not necessarily reflect the actual decision outcome.

3.7. *Illusion of control*

In a series of studies, Brandimarte et al. (2013) dealt with the hypothesis that users suffer from an 'illusion of control' when dealing with the privacy of their data. They found that users indeed seem to confuse the control over the publication of information with the control over the assessment of that information by third parties. Therefore, users are more likely to allow the publication of personal information and even provide more sensitive information, if they are given explicit control over the publication of their data. If, on the other hand, a third party is responsible for the publication of the same data, users may perceive a loss of control and express concerns about the usage of their data by others without authorization (Brandimarte et al., 2009). According to this hypothesis, the paradoxical behavior is caused by the false feeling of control over the further usage of personal data, which occurs if users can initially decide over the publication of it (e.g., by posting in social networks and managing the privacy settings for the post).

Table 1 – Predictor variables for privacy attitude.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns			
For informational privacy	Dienlin and Trepte (2015)	0.42***	SEM
For social privacy		0.33***	
For psychological privacy		0.25***	

***p < .001.

Table 2 – Predictor variables for social scientist's attitude towards data sharing.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived career benefit	Kim and Adler (2015)	0.36***	SEM
Perceived career risk	Kim and Adler (2015)	−0.18***	SEM

***p < .001.

Table 3 – Predictor variables for attitude towards an information practice.

Predictor variable	Primary study	Effect size (β)	Coefficient
Concern for information privacy	Schwaig et al. (2013)	−0.70***	SEM
Computer anxiety	Schwaig et al. (2013)	−0.70***	SEM
Permission granted	Schwaig et al. (2013)	0.66***	SEM
Consumer alienation	Schwaig et al. (2013)	−0.61***	SEM
Interaction with IT	Schwaig et al. (2013)	0.52***	SEM
Self-esteem	Schwaig et al. (2013)	0.51***	SEM
Transfer internally	Schwaig et al. (2013)	0.51***	SEM

***p < .001.

3.8. *The privacy paradox as methodological artefact*

Another potential reason for the dichotomy between behavior and attitude is based on methodological considerations. One explanation may be the inappropriate operationalization of these constructs in the particular studies dealing with the privacy paradox (Dienlin and Trepte, 2015). Behavior is often assessed as a dichotomous answer (for example by asking if someone has a public Facebook profile or not), whereas attitude is measured on a metric (e.g., a Likert-based) scale. However, dichotomous data always implies a potential limitation of variance, which can in turn lead to a reduction of statistical power. Hence, it is possible that in fact there is a strong relationship between attitude and behavior and previous studies just failed to verify this relationship due to their inappropriate operationalization.

Another approach is based on the assumption of a multidimensional nature of privacy. Dienlin and Trepte (2015) suggest that it is important to distinguish between privacy attitudes and privacy concerns on the one hand, and between informational, social and psychological privacy on the other hand. Indeed, a corresponding study by Dienlin and Trepte (2015), which accounts for these different facets of privacy revealed an indirect effect of privacy concerns on privacy behavior. Specifically, privacy concerns had an effect on privacy attitudes, which in turn influenced privacy intentions, which finally influenced privacy behavior.

So far, no definite explanation for the privacy paradox has been proposed. However, considering the variety of possible explanations for the privacy paradox, either interpreting the phenomenon or developing extensive models to shed light on it, the dichotomy between privacy attitudes, concerns or perceived risk and privacy behavior should not be perceived as paradox anymore. To further understand which factors relate to user privacy, we report the standardized effect size (β) that could be found in the included studies concerning the association of the different predictor variables with privacy attitude, privacy concern, perceived privacy risk, privacy intention and privacy behavior in the next section.

4. Empirical privacy paradox explanation attempts

This section focuses on empirical attempts to explain the privacy paradox by investigating the factors that significantly predict privacy attitude, concerns, perceived risk, behavioral intention and behavior. To identify how important these factors are for the prediction of the different privacy aspects, we will report the standardized effect sizes (β) found in the included studies for the various predictor variables (Tables 1–33). Effect sizes will be interpreted as small ($\beta = 0.10$), medium ($\beta = 0.30$) or large ($\beta = 0.50$), as suggested by Cohen (1988) for Pearson's correlation coefficient. Only statistically significant results are considered. Significance is presented together with the corresponding effect size, with one asterisk indicating significance on a 5% level ($p < .05$), two asterisks on a 1% level ($p < .01$), and three asterisks on a 0.1% level ($p < .001$). Where path analyses lack sufficient statistical power (< 0.8), a '(i.p.) is included in the effect size column. Predictor variables are

Table 4 – Predictor variables for attitude towards social network games.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived security	Shin and Shin (2011)	0.50***	SEM
Perceived playfulness	Shin and Shin (2011)	0.47***	SEM

***p < .001.

Table 5 – Predictor variables for attitude towards location-based social network applications.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived benefit	Koohikamali et al. (2015)	0.50***	SEM
Perceived risk	Koohikamali et al. (2015)	−0.37***	SEM
Social norm	Koohikamali et al. (2015)	0.14** (i.p.)	SEM
Opinion leadership	Koohikamali et al. (2015)	0.08* (i.p.)	SEM

*p < .05.
**p < .01.
***p < .001.

Table 6 – Predictor variables for attitude towards a location-based mobile website.

Predictor variable	Primary study	Effect size (β)	Coefficient
Trust	Zhang et al. (2014)	0.79**	SEM

**p < .01.

Table 7 – Predictor variables for general privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Consumer alienation	Schwaig et al. (2013)	0.60***	SEM
Self-esteem	Schwaig et al. (2013)	−0.54***	SEM
Perceived risk	Liao et al. (2011)	0.44***	SEM
Computer anxiety	Schwaig et al. (2013)	0.37***	SEM
Disposition to privacy	Li (2014a)	0.36***	SEM
Social awareness	Liao et al. (2011)	0.20***	SEM
Gender	Abbas and Mesch (2015)	0.17**	Regression
Internet anxiety	Li (2014a)	0.17* (i.p.)	SEM
General willingness to share	Taddicken (2014)	−0.15***	SEM
Internet literacy	Liao et al. (2011)	0.14**	SEM
Culture - collectivism	Abbas and Mesch (2015)	0.10* (i.p.)	Regression

*p < .05.
**p < .01.
***p < .001.

Table 8 – Predictor variables for website specific privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived privacy risk	Xu et al. (2013)	0.69**	SEM
Website reputation	Li (2014a)	−0.20** (i.p.)	SEM
	Li (2014b)	−0.28**	SEM
For high reputation websites		−0.26**	
For low reputation websites		−0.45**	
Disposition to privacy	Li (2014a)	0.23* (i.p.)	SEM
	Li (2014b)	0.20* (i.p.)	SEM
For high reputation websites		0.20* (i.p.)	
For low reputation websites		0.26** (i.p.)	
Website familiarity	Li (2014b)	−0.20** (i.p.)	SEM
For high reputation websites		−0.20** (i.p.)	
Information control	Xu et al. (2013)	−0.20** (i.p.)	SEM
Existence of a security cue	Zhang et al. (2014)	0.20* (i.p.)	SEM

*p < .05.
**p < .01.

Table 9 – Predictor variables for context specific privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived control	Xu et al. (2012)	−0.60**	SEM
Industry self-regulation	Xu et al. (2012)	−0.19**	SEM
Privacy experience	Xu et al. (2012)	0.16* (i.p.)	SEM

*p < .05.
**p < .01.

Table 10 – Predictor variables for health information privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived health information sensitivity	Bansal et al. (2010)	0.28***	SEM
Previous online privacy invasion	Bansal et al. (2010)	0.17***	SEM

***p < .001.

Table 11 – Predictor variables for teenage privacy concerns on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived ease of privacy control	Jia et al. (2015)	−0.18*** (i.p.)	SEM
SNS use frequency	Jia et al. (2015)	0.14** (i.p.)	SEM
	Feng and Xie (2014)	0.12** (i.p.)	SEM
Parental privacy concern	Wisniewski et al. (2015)	0.13** (i.p.)	SEM
	Feng and Xie (2014)	0.12** (i.p.)	SEM
Risky interaction	Jia et al. (2015)	0.10* (i.p.)	SEM
	Wisniewski et al. (2015)	0.10* (i.p.)	SEM

*p < .05.
**p < .01.
***p < .001.

Table 12 – Predictor variables for perceived privacy risk.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns	Miltgen et al. (2013)	0.34***	SEM
	Zhou (2015)	0.23**	SEM
	Li et al. (2011)	0.22***	SEM
	Keith et al. (2013)	0.18***	SEM
Level of trust in the recipient's ability to protect data	Beldad et al. (2011)	−0.32***	Regression
Personalization	Xu et al. (2011)	0.29**	SEM
Perceived relevance of information	Li et al. (2011)	−0.28***	SEM
Perceived privacy regulatory protection	Miltgen and Smith (2015)	−0.25***	SEM
Privacy risk awareness	Keith et al. (2013)	0.25***	SEM
Initial joy	Li et al, (2011)	−0.21***	SEM
Prior experience with privacy infringement	Xu et al. (2011)	0.20**	SEM
	Bansal et al. (2010)	0.17***	SEM
	Baek and Kim (2014)	0.08***	Regression
Assessment of data sensitivity			
for publicly accessible contact data	Beldad et al. (2011)	0.18*	Regression
for confidential data		0.19**	
Initial fear	Li et al. (2011)	0.17* (i.p.)	SEM
Trust	Zhou (2015)	−0.15*	SEM
	Miltgen and Smith (2015)	−0.10**	SEM
Age	Baek and Kim (2014)	−0.10***	Regression
Gender	Baek and Kim (2014)	0.02* (i.p.)	Regression
Maternalistic personality	Baek and Kim (2014)	0.11**	Regression

*p < .05.
**p < .01.
***p < .001.

Table 13 – Predictor variables for general intention to disclose information.

Predictor variable	Primary study	Effect size (β)	Coefficient
Website trust	Bansal et al. (2010)	0.85***	SEM
	Li (2014a)	0.42***	SEM
	Wakefield (2013)	0.23**	SEM
Website privacy concern	Li (2014a)	−0.43***	SEM
Perceived privacy risk	Keith et al. (2013)	−0.42***	SEM
	Li et al. (2011)	−0.37**	SEM
	Norberg et al. (2007)	−0.34*	Regression
Privacy concern	Bansal et al. (2010)	−0.27***	SEM
	Li et al. (2011)	−0.15* (i.p.)	SEM
	Keith et al. (2013)	−0.07** (i.p.)	SEM
Privacy protection belief	Wakefield (2013)	0.26***	SEM
	Li et al. (2011)	0.19*	SEM
Perceived benefits	Keith et al. (2013)	0.22***	SEM
Positive affect (enjoyment)	Wakefield (2013)	0.19**	SEM
Negative affect	Wakefield (2013)	−0.11* (i.p.)	SEM
Prior positive experience with the website	Bansal et al. (2010)	0.08** (i.p.)	SEM
Employment	Keith et al. (2013)	0.07** (i.p.)	SEM

*p < .05.
**p < .01.
***p < .001.

Table 14 – Predictor variables for intention to disclose information on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived benefit	Xu et al. (2013)	0.81***	SEM
	Xu et al. (2013)	0.81***	Regression
Willingness	Van Gool et al. (2015)	0.34***	SEM
Attitude	Van Gool et al. (2015)	0.32***	SEM
Privacy concerns	Xu et al. (2013)	−0.19* (i.p.)	SEM
	Xu et al. (2013)	−0.14** (i.p.)	Regression
Subjective norm of friends	Van Gool et al. (2015)	0.17***	SEM
Subjective norm of parents	Van Gool et al. (2015)	0.15***	SEM
Gender	Van Gool et al. (2015)	0.11***	SEM
Age	Van Gool et al. (2015)	0.07*	SEM

*p < .05.
**p < .01.
***p < .001.

Table 15 – Predictor variables for intention to make Facebook data publicly accessible.

Predictor variable	Primary study	Effect size (β)	Coefficient
Need for consent			
For activity data	Knijnenburg et al. (2013)	−0.25***	Regression
For location data		−0.14*	
For contact data		−0.58***	
Trust in Facebook			
For activity data	Knijnenburg et al. (2013)	0.30***	Regression
For location data		0.33***	
For contact data		0.28***	
For interests data		0.49***	
Knowledge about privacy policy			
For location data	Knijnenburg et al. (2013)	−0.10* (i.p.)	Regression
For interests data		−0.16***	

*p < .05.
***p < .001.

Table 16 – Predictor variables for intention to disclose data to an online retailer.

Predictor variable	Primary study	Effect size (β)	Coefficient
Collection concerns			
For health data	Knijnenburg et al. (2013)	−0.16* (i.p.)	Regression
For contact data		−0.45***	
For interests data		−0.21*	
For work data		−0.27***	
Control concerns			
For interests data	Knijnenburg et al. (2013)	0.23*	Regression
For work data		0.23*	

*p < .05.
***p < .001.

Table 17 – Predictor variables for willingness to disclose information.

Predictor variable	Primary study	Effect size (β)	Coefficient
Liked targeted ads			
For browsing information	Leon et al. (2013)	0.68***	Regression
For computer information		0.59***	
For demographic information		0.62***	
For location information		0.62***	
For personally identifiable information		0.62***	
Perceived value			
For covert-based scenario	Xu et al. (2011)	0.60**	SEM
For overt-based scenario		0.56**	
Retention period: indefinite			
For browsing information	Leon et al. (2013)	−0.47***	Regression
For demographic information		−0.17*	
For location information		−0.28***	
Privacy concerns	Lee and Cranage (2011)	−0.41***	Regression
For browsing information	Leon et al. (2013)	−0.29***	Regression
For computer information		−0.25***	
For demographic information		−0.33***	
For location information		−0.34***	
For personally identifiable information		−0.26***	
Perceived usefulness	Lee and Cranage (2011)	0.33***	Regression
Usage scope: health site and Facebook			
For location information	Leon et al. (2013)	−0.33***	Regression
For personally identifiable information		−0.33***	
Usage scope: all sites			
For browsing information	Leon et al. (2013)	−0.30***	Regression
Facebook usage			
For browsing information	Leon et al. (2013)	0.15***	Regression
For computer information		0.22***	
For demographic information		0.21***	
For location information		0.19***	
For personally identifiable information		0.19***	
Personal innovativeness			
For covert-based scenario	Xu et al. (2011)	0.19**	SEM
For overt-based scenario		0.11* (i.p.)	
Coupon proneness			
For covert-based scenario	Xu et al. (2011)	0.15** (i.p.)	SEM
Age			
For demographic information	Leon et al. (2013)	−0.004*	Regression
For location information		−0.008***	

*p < .05.
**p < .01.
***p < .001.

Table 18 – Predictor variables for willingness to disclose information about peer relationships on Facebook.

Predictor variable	Primary study	Effect size (β)	Coefficient
Prototype similarity	Van Gool et al. (2015)	0.32***	SEM
Prototype favorability	Van Gool et al. (2015)	0.21***	SEM
Attitude	Van Gool et al. (2015)	0.13***	SEM
Gender	Van Gool et al. (2015)	0.11***	SEM
Age	Van Gool et al. (2015)	0.07*	SEM

*p < .05.
***p < .001.

Table 19 – Predictor variables for general information disclosure.

Predictor variable	Primary study	Effect size (β)	Coefficient
General Willingness to Self-disclose	Taddicken (2014)	0.59***	SEM
Number of applications	Taddicken (2014)	−0.35***	SEM
Ads awareness	Wang et al. (2015)	−0.28***	SEM
Social relevance	Taddicken (2014)	0.27***	SEM
Existence of a security cue (certificate warning)	Zhang et al. (2014)	0.14*	SEM
Comfort level in disclosing information	Wang et al. (2015)	0.13*	SEM
Intent to disclose	Keith et al. (2013)	0.12**	SEM
Control over what information is used for	Wang et al. (2015)	−0.12**	SEM
Age	Taddicken (2014)	−0.02*** (i.p.)	SEM

*p < .05.
**p < .01.
***p < .001.

Table 20 – Predictor variables for information disclosure on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy intention			
Informational privacy	Dienlin and Trepte (2015)	−0.65***	SEM
Psychological privacy		−0.79***	
Privacy concerns	Becker and Pousttchi (2012)	−0.43***	SEM
Privacy attitude			
Informational privacy	Dienlin and Trepte (2015)	−0.11*	SEM
Psychological privacy		−0.08* (i.p.)	

*p < .05.
***p < .001.

listed in descending order according to the respective effect sizes, i.e., the best predictor is always reported first and the worst predictor last. The reported effect sizes are either retrieved from regression analyses or structural equation modeling. Thus, the corresponding type of coefficient is reported in the last column, with 'SEM' referring to effect sizes from structural equation modeling and 'Regression' to those from regression analyses.

4.1. *Privacy attitude, privacy concerns and perceived privacy risk*

The theoretical construct 'attitude towards privacy' actually refers to the general appraisal of different privacy behaviors. However, it is often assessed as 'privacy concerns' or 'perceived privacy risk'. Since the relationship between attitude, concerns and perceived risk is not clearly defined in the literature, we will deal with the constructs separately.

4.1.1. *Attitude*

Some of the included studies actually assessed privacy attitude, i.e., the more general evaluation of a certain privacy behavior or privacy relevant product, instead of more specific privacy concerns or perceived privacy risk. Dienlin and Trepte (2015) differentiate three aspects of privacy attitude, Kim and Adler (2015) focused on social scientists' attitude towards sharing research data and Schwaig et al. (2013) investigated users' attitude towards the information practice of corporations. Other studies assessed specific privacy attitudes, namely towards social network games, location-based social network applications and a location-based mobile website.

4.1.1.1. *Privacy attitude* In their study, Dienlin and Trepte (2015) distinguish between three different privacy concepts: (1) Informational privacy, i.e., (not) giving identifiable information on Facebook, (2) social privacy, i.e., restricting access to one's Facebook profile, and (3) psychological pri-

Table 21 – Predictor variables for information disclosure on SNS (breadth).

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns	Becker and Pousttchi (2012)	−0.43***	SEM
Gender	Li et al. (2015)	−0.18** (i.p.)	SEM
For young users (< 24)		−0.21**	
For middle-aged users (25–39)		−0.20**	
For older users (> 40)		−0.19* (i.p.)	
User activeness and experience on SNS			
For older users (> 40)	Li et al. (2015)	0.07* (i.p.)	SEM
Age	Li et al. (2015)	−0.04*	SEM
For male users		−0.05* (i.p.)	
For female users		−0.05* (i.p.)	
Number of posted blogs	Li et al. (2015)	0.01** (i.p.)	SEM
For male users		0.01** (i.p.)	
For female users		0.01** (i.p.)	
For young users (< 24)		0.01** (i.p.)	
For middle-aged users (25–39)		0.01** (i.p.)	
For older users (> 40)		0.01** (i.p.)	
Number of friends			
For female users	Li et al. (2015)	0.01* (i.p.)	SEM

*p < .05.
**p < .01.
***p < .001.

Table 22 – Predictor variables for information disclosure on SNS (depth).

Predictor variable	Primary study	Effect size (β)	Coefficient
Gender	Li et al. (2015)	−0.20** (i.p.)	SEM
For young users (< 24)		−0.25**	
For middle-aged users (25–39)		−0.20**	
Age	Li et al. (2015)	−0.03* (i.p.)	SEM
For female users		−0.03*(i.p.)	
User activeness and experience on SNS			
For older users (> 40)	Li et al. (2015)	−0.03* (i.p.)	SEM
Number of friends			
For female users	Li et al. (2015)	0.01* (i.p.)	SEM
Number of posted blogs	Li et al. (2015)	0.01* (i.p.)	SEM

*p < .05.
**p < .01.

Table 23 – Predictor variables for information disclosure on SNS (less sensitive information).

Predictor variable	Primary study	Effect size (β)	Coefficient
Gender	Li et al. (2015)	−0.17** (i.p.)	SEM
For young users (< 24)		−0.17** (i.p.)	
For middle-aged users (25–39)		−0.16** (i.p.)	
For older users (> 40)		−0.15* (i.p.)	
User activeness and experience on SNS			
For older users (> 40)	Li et al. (2015)	0.07* (i.p.)	SEM
Age	Li et al. (2015)	−0.04* (i.p.)	SEM
For male users		−0.04* (i.p.)	
For female users		0.05* (i.p.)	
Number of posted blogs	Li et al. (2015)	0.01** (i.p.)	SEM
For male users		0.01** (i.p.)	
For female users		0.01** (i.p.)	
For young users (< 24)		0.01** (i.p.)	
For middle-aged users (25–39)		0.01** (i.p.)	
For older users (> 40)		0.01** (i.p.)	
Number of friends			
For female users	Li et al. (2015)	0.01* (i.p.)	SEM

*p < .05.
**p < .01.

Table 24 – Predictor variables for teenage information disclosure on social media.

Predictor variable	Primary study	Effect size (β)	Coefficient
Intention			
For peer relationship information	Van Gool et al. (2015)	0.58***	SEM
Basic information disclosure			
For sensitive information	Wisniewski et al. (2015)	0.29***	SEM
Network size/ Number of friends			
For contact information	Xie and Kang (2015)	0.21***	Regression
For insensitive information		0.24***	
SNS complexity			
For personal information	Jia et al. (2015)	0.20***	SEM
For sensitive information		0.23***	
SNS use frequency			
For personal information	Jia et al. (2015)	0.21***	SEM
	Xie and Kang (2015)	0.10* (i.p.)	Regression
For sensitive information	Jia et al. (2015)	0.17*** (i.p.)	SEM
Willingness			
For peer relationship information	Van Gool et al. (2015)	0.17***	SEM
Gender	Jia et al. (2015)	−0.12** (i.p.)	SEM
For contact information	Xie and Kang (2015)	−0.16***	Regression
For peer relationship information	Van Gool et al. (2015)	0.17***	SEM
Age	Jia et al. (2015)	0.16** (i.p.)	SEM
For personal information	Xie and Kang (2015)	0.15**	Regression
For peer relationship information	Van Gool et al., 2015)	0.06*	SEM
Privacy settings			
For contact information	Xie and Kang (2015)	−0.10* (i.p.)	Regression
For insensitive information		−0.14**	
Parental direct intervention	Wisniewski et al. (2015)	−0.13** (i.p.)	SEM
Having SNS friends that do not go to school with the participant			
For personal information	Xie and Kang (2015)	0.10*	Regression
Having strangers as SNS friends			
For contact information	Xie and Kang (2015)	0.13*	Regression
For insensitive information		0.12*	
Trust in other people			
For contact information	Xie and Kang (2015)	0.10*	Regression

*p < .05.
**p < .01.
***p < .001.

Table 25 – Predictor variables for information disclosure towards a mobile app recommender.

Predictor variable	Primary study	Effect size (β)	Coefficient
Collection concerns			
For context data	Knijnenburg et al. (2013)	0.46***	Regression
For demographic data		0.22***	
Mobile internet usage			
For context data	Knijnenburg et al. (2013)	0.25***	Regression
For demographic data		0.15*	

*p < .05.
***p < .001.

vacy, i.e., (not) communicating personal information on Facebook. Privacy concerns regarding informational privacy are a mediocre to good predictor for informational privacy attitude, whereas social privacy concerns moderately predict social privacy attitude and psychological privacy concerns weak to moderately predict psychological privacy attitude.

4.1.1.2. Social scientist's attitude towards data sharing Social scientist's attitude towards sharing research data is moderately predicted by the subjectively gained career benefit and rather weakly by the perceived career risk.

4.1.1.3. Attitude towards an information practice The information practice of a corporation describes the procedure the corporation follows in the handling of a consumer's personal information. The consumer's attitude towards this information practice is very well predicted by his/her concern for information privacy and computer anxiety. Other good predictors are whether s/he has granted the corporation permission to use his/her personal data, the feeling of consumer

Table 26 – Predictor variables for location disclosure on location-based social network application.

Predictor variable	Primary study	Effect size (β)	Coefficient
Attitude towards location-based social network application	Koohikamali et al. (2015)	0.43***	SEM
Incentives	Koohikamali et al. (2015)	0.11* (i.p.)	SEM

*p < .05.
***p < .001.

Table 27 – Predictor variables for sharing of profile information in a mobile app.

Predictor variable	Primary study	Effect size (β)	Coefficient
Intent to disclose	Keith et al. (2013)	0.13***	SEM

***p < .001.

Table 28 – Predictor variables for usage of a location sharing application.

Predictor variable	Primary study	Effect size (β)	Coefficient
Benefits – entertainment	Beldad and Citra Kusumadewi (2015)	0.32***	Regression
Social influence	Beldad and Citra Kusumadewi (2015)	0.21***	Regression
Intent to disclose	Keith et al. (2013)	0.18***	SEM
Benefits – impression management	Beldad and Citra Kusumadewi (2015)	0.15***	Regression
Competence-based trust in LSA	Beldad and Citra Kusumadewi (2015)	0.14***	Regression
General trust in LSA network	Beldad and Citra Kusumadewi (2015)	0.11**	Regression

**p < .01.
***p < .001.

Table 29 – Predictor variables for usage of social network games.

Predictor variable	Primary study	Effect size (β)	Coefficient
Usage intention	Shin and Shin (2011)	0.39*	SEM

*p < .05.

Table 30 – Predictor variables for privacy settings on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy intention			
For informational privacy	Dienlin and Trepte (2015)	0.65***	SEM
For social privacy		0.45***	
For psychological privacy		0.79***	
Privacy concerns			
For Hyves, random sample	Utz and Kramer (2009)	0.35**	Regression
For Hyves, self selected sample		0.29***	
For StudiVZ		0.21**	
Perceived norms regarding what to show only to friends			
For Hyves, random sample	Utz and Kramer (2009)	0.33**	Regression
For StudiVZ		0.31**	
Impression management			
For Hyves, self selected sample	Utz and Kramer (2009)	0.22**	Regression
Privacy attitude			
For informational privacy	Dienlin and Trepte (2015)	0.11* (i.p.)	SEM
For social privacy		0.20***	
For psychological privacy		0.08* (i.p.)	
Narcissism			
For StudiVZ	Utz and Kramer (2009)	−0.16* (i.p.)	Regression

*p < .05.
**p < .01.
***p < .001.

Table 31 – Predictor variables for teenage privacy settings on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns about their online data being collected by marketers			
Implementation of privacy-setting strategies	Feng and Xie (2014)	0.17***	SEM
Teenage level of SNS use		0.10* (i.p.)	

*p < .05.
***p < .001.

Table 32 – Predictor variables for privacy-protective behaviors.

Predictor variable	Primary study	Effect size (β)	Coefficient
Years of internet experience			
Technical behavior	Park (2015)	0.25***	SEM
Social behavior		0.21***	
Comparative optimism toward young users	Baek and Kim (2014)	0.24**	Regression
Perceived rewards for data disclosure	Miltgen and Smith (2015)	−0.24***	SEM
Privacy risk concerns	Miltgen and Smith (2015)	0.23***	SEM
Internet use			
Technical behavior	Baek and Kim (2014)	0.11*	Regression
Social behavior	Park (2015)	0.11* (i.p.)	SEM
		0.21***	
Gender	Baek and Kim (2014)	−0.04** (i.p.)	Regression
Technical behavior	Park (2015)	−0.19***	SEM
Autonomy			
Technical behavior	Park (2015)	0.15**	SEM
Age			
Technical behavior	Park (2015)	−0.14**	SEM
Social behavior		−0.15**	
Perceived personal risk	Baek and Kim (2014)	0.14**	Regression
Household income			
Social behavior	Park (2015)	−0.13*	SEM

*p < .05.
**p < .01.
***p < .001.

alienation (i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices), whether the consumer generally interacts with IT, the level of the consumer's self-esteem and whether the corporation only transfers the information internally.

4.1.1.4. *Attitude towards social network games* Both perceived security and perceived playfulness of a social network game are relatively good predictors for the user's attitude towards such games.

4.1.1.5. *Attitude towards location-based social network applications* The attitude towards location-based social network applications is predicted well and moderately to well by the perceived benefit and risk associated with using the application, respectively. Weak predictors are the social norm towards the application and the degree to which the user sees his-/herself as opinion leader, i.e., someone whose opinion influences others to make decisions.

4.1.1.6. *Attitude towards a location-based mobile website* The attitude towards a fictitious mobile website which provides restaurant recommendations based on the users current location is very well predicted by the user's trust towards that website.

4.1.2. *Privacy concerns*

We further divide the construct 'privacy concerns' due to different operationalization in the corresponding studies, which assessed general privacy concerns, but also website and context specific privacy concerns, health information privacy concerns, and privacy concerns of teenagers relating to the use of social network sites (SNS).

4.1.2.1. *General privacy concerns* General privacy concerns is best predicted by the feeling of consumer alienation, i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices. Furthermore, low levels of self-esteem are strongly associated with the expression of privacy concerns. High levels of perceived risk, computer anxiety and a strong disposition to privacy moderately predict high values of general privacy concerns. A small predictive value was shown for social awareness (i.e., passive involvement and raised interest in social issues), gender, with female users expressing higher levels of concerns, internet anxiety, internet literacy, the general willingness to share data on the internet

Table 33 – Predictor variables for teenage privacy protection on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Risky interaction			
Remedy of disclosure	Jia et al. (2015)	0.44***	SEM
	Wisniewski et al. (2015)	0.46***	
Privacy concern			
Remedy of disclosure	Jia et al. (2015)	0.23***	SEM
	Wisniewski et al. (2015)	0.10**	
Advice seeking	Jia et al. (2015)	0.36***	
	Wisniewski et al. (2015)	0.19***	
Sensitive disclosure			
Remedy of disclosure	Jia et al. (2015)	0.14***	SEM
	Wisniewski et al. (2015)	0.12***	
Advice seeking	Jia et al. (2015)	0.20***	
Gender			
Remedy of disclosure	Jia et al. (2015)	0.16***	SEM
Advice seeking		0.10*	
Advice-Seeking			
Remedy of disclosure	Wisniewski et al. (2015)	0.12***	SEM
Age			
Advice seeking	Jia et al. (2015)	−0.11**	SEM
Parental direct intervention			
Remedy of disclosure	Wisniewski et al. (2015)	−0.10*	SEM
Advice seeking		−0.10*	
Parental active mediation			
Remedy of disclosure	Wisniewski et al. (2015)	0.10**	SEM
SNS frequency			
Remedy of disclosure	Jia et al. (2015)	0.08*	SEM

*p < .05.
**p < .01.
***p < .001.

and cultural factors, with users from collectivistic cultures being more concerned.

4.1.2.2. *Website specific privacy concerns* Like for general privacy concerns, for the prediction of website specific privacy concerns the perceived risk plays an important role as well. The particular website's reputation is found to be important especially if it holds a low reputation; however, this effect does not occur for the variable 'disposition to privacy', which is a small to moderate predictor for website privacy concerns for all kinds of website reputations. Users tend to be less concerned if the website is familiar to them, they feel that they can control how their released information is processed and if the website does not contain a security cue, which warns users about untrusted site security authorization.

4.1.2.3. *Context specific privacy concerns* Analog to the prediction of general privacy concerns by consumer alienation, the control users perceive about the processing of their data is a crucial factor for the prediction of context specific privacy concerns, with users who feel less in control expressing more privacy concerns. Users also tend to be more concerned if they had experienced an infringement of their privacy before, whereas the presentation of the TRUSTe seal, showing the membership in an industry self-regulated privacy association, combined with the URL link to the according privacy policy, is related with less privacy concerns. Both predictor values can be considered as small to medium.

4.1.2.4. *Health information privacy concerns* The sensitivity of the particular health information moderately predicts the respective privacy concerns. The predictive value of previous privacy invasions, however, ranges between small and medium.

4.1.2.5. *Teenage privacy concerns on SNS* Again, the variable best predicting privacy concerns, in this particular case experienced by teenagers concerning their use of social networks, is associated with perceived control: Teenagers are found to hold more privacy concerns if they find it difficult to control their privacy. However, this effect is considerably lesser than for context specific and general privacy concerns. Other variables that predict the extend of privacy concerns somewhat are the frequency of social network use, the existence of parental privacy concerns and the general performance of social risky interactions, with higher values predicting more privacy concerns.

4.1.3. *Perceived privacy risk*

None of the examined variables was found to be of great significance for the prediction of perceived privacy risk. The predictive power of privacy concerns varies across different studies from small to medium, but was found to be smaller than for the corresponding prediction of privacy concerns by perceived risk. How much risk is perceived is further moderately predicted by the user's trust in the recipient's ability to protect his/her data, the degree of personalization that is gained by data disclosure and the perceived relevance of the collected

information. Furthermore, negative values of perceived privacy regulatory protection (which refers to the user's perception of provisions and systems that protect his/ her personal data, in terms of existence and adequacy) were found to predict an increase of the perceived privacy risk. In accordance with that, users perceive less risk if they trust for example the governmental and commercial entities that are associated with information privacy, if they have an initial joyful emotional reaction at the first impression of the data receiving website, as well as if they are younger and male, though the last-mentioned effect was negligible. On the other hand, users perceive higher privacy risk if they are well aware of privacy risks in general, if they have already experienced privacy infringements, if the respective data is rather sensitive, if their first emotional reaction to the receiving website is fearful and, finally, if they have a maternalistic personality, meaning they have a strong desire to protect the socially vulnerable from external danger.

4.2. *Privacy related behavioral intention and willingness*

We will distinguish between the 'intention' and the 'willingness' to disclose data, since it is not specified in the literature whether these concepts can be considered as similar.

4.2.1. *Intention*

Due to different operationalization in the included studies, we will report the predictor values separately for the general intention to disclose information, the intention to disclose information on social network sites (SNS), the intention to make Facebook data publicly (i.e., beyond the social network) accessible and the intention to disclose data to an online retailer.

4.2.1.1. *General intention to disclose information* The general intention to disclose information can be very well predicted by the user's trust in the receiving website according to Bansal et al. (2010), slightly better than moderately according to Li (2014a) and moderately to weakly according to Wakefield (2013). Likewise, high values of privacy protection belief, i.e., the belief that one is able to control how the disclosed information is used moderately to weakly predict an increase in intention to disclose information. High values of perceived privacy risk, on the other hand, moderately predict a decrease in the intention to disclose information, along with high values of website privacy concern and, to a lesser extent, general privacy concern. A small to moderate predictive effect was also found for the perceived benefits gained through information disclosure and the experience of a positive affect. Experiencing a negative affect, the prior experience with the receiving website and the number of years a person has spent in full-time employment (regardless which kind of job s/he holds) also somewhat predict the disclosure intention.

4.2.1.2. *Intention to disclose information on SNS* The benefits users expect to gain from the disclosure of their data are an excellent predictor of their intention to disclose information on SNS. Moderate predictive power could be shown for the attitude towards disclosure and the willingness to disclose. The small predictive effect of gender found by Van Gool et al. (2015) suggests that female adolescents have a higher intention to self-disclose. The same goes for older adolescents and those whose friends and parents have a positive attitude towards data disclosure on social networks. Privacy concerns, on the other hand, are somewhat negatively associated with the intention to disclose information on social networks.

4.2.1.3. *Intention to make Facebook data publicly accessible* The intention to make Facebook data publicly accessible, that is, to share the answer to various Facebook items with 'everyone on the internet', is best predicted by different variables, depending on the type of information. The trust someone has in Facebook mostly predicts his/her intention to share interests data, whereas the need for consent (i.e., the belief that Facebook should only share data or make changes in its settings with the permission of the user) is strongly associated with the intention to share contact data, rather moderately with the intention to share activity data, only weakly with the disclosure of location data and not significantly with the disclosure of interests data at all. At the same time, knowledge about privacy policies does not predict the disclosure of location or contact data, and only marginally predicts the disclosure of interests and activity data.

4.2.1.4. *Intention to disclose data to an online retailer* Like the intention to disclose Facebook data to the public, the intention to disclose information to an online retailer (e.g., for registration purposes) is predicted by different variables according to the particular type of disclosed information. The absence of collection concerns (i.e., general concerns about online companies collecting data) is strongly associated with the intention to disclose contact data, but there is only a weak relationship for health data. Control concerns, that is, a strong desire to control the processing of one's own personal data, is a weak to moderate predictor of the disclosure intention for interests and work data, but not for health or contact data.

4.2.2. *Willingness*

We report the predictor values for general willingness to disclose information and willingness to disclose information about peer relationships on Facebook.

4.2.2.1. *Willingness to disclose information* Many variables were found to predict the willingness to disclose information in general. In line with the privacy calculus model, the user's decision to disclose information is strongly associated with the perceived value or benefits they can gain through that disclosure (e.g., the 'perceived value', the 'perceived usefulness' or the fact that they 'liked the targeted ads'). This applies to both cases, the situation in which the benefits (e.g., personalization) are overt ('overt-based') or hidden ('covert-based'). Users are unwilling to share browsing information if the data storage retention period is indefinite; however, this circumstance is less important for the disclosure of demographic information. Privacy concerns are likely to be moderate predictors for the willingness to disclose information, irrespective of the information type. Facebook users tend to exhibit a greater willingness to disclose information ('Facebook usage'), and also do users who are personally innovative (e.g.,

early adopters) or prone to discounts (e.g., coupons). In contrast, users are less willing to disclose information if these are shared with third parties, for example Facebook, and not only with the recipient ('usage scope'; in Leon et al. (2013) the recipient is a health site). Age, on the other hand, was shown to be a negligible predictor for the willingness to disclose information.

4.2.2.2. Willingness to disclose information about peer relationships on Facebook How willing teenagers are to disclose information about their peer relationships on Facebook is moderately predicted by the mental prototype they have of a person who performs this very behavior. If they perceive the prototype, that is, the typical person who would disclose information about peer relationships on Facebook, as similar to them and also evaluate the prototype as positive, they are more willing to disclose peer relationship information on Facebook themselves. The attitude towards disclosure, gender and age are of lesser, but still statistically significant predictive power for the willingness to disclose, with female and older adolescents being more willing to disclose.

4.3. *Privacy related behavior*

The examined privacy behavior comprises the disclosure of information, either in general, on a social network or towards a particular application, as well as the actual usage of data sharing applications, the management of privacy settings and the performance of privacy protection behavior.

4.3.1. *Information disclosure*

The operationalization of information disclosure in the included studies comprises general information disclosure, information disclosure on social network sites (SNS), the breadth and depth of information disclosure on SNS, the disclosure of less sensitive information on SNS, teenager's information disclosure on social media, information disclosure towards a recommender application for mobile apps, the disclosure of location information on a location-based social network application and the sharing behavior regarding personal profile information in a mobile application.

4.3.1.1. General information disclosure Whether someone tends to disclose information in general was found to be highly associated with his/her willingness to self-disclose in the first place. The association between behavioral intention and actual disclosure might be much smaller. A moderate association was found for the perceived relevance of the social web in the user's social environment, the number of social web applications used (with users who use only a few applications tending to disclose more information overall) and the awareness of how the disclosed information is used (in the case of the study conducted by Wang et al. (2015), for personalized advertising). A small negative association was found for the control over what the disclosed information is used for, the experienced comfort during information disclosure and the existence of a security cue on the receiving website in form of a banner warning that a trusted security certificate could not be detected. Albeit contra intuitive at the first glance, the negative association between information disclosure and control about the further processing of the disclosed information may be caused by an increase in awareness about potential consequences, which is in turn triggered by the theoretical preoccupation with the processing of personal information. A marginal predictive effect was found for age.

4.3.1.2. Information disclosure on SNS The privacy intention, i.e., the intention users have concerning the respective disclosure behavior, was shown to be the main variable predicting information disclosure on SNS in general, with a greater predictive power for psychological privacy behavior (that is, how personal is the social network profile and how many personal things are posted there) than for informational privacy behavior (the amount of identifying information that can be found on the SNS). Furthermore, a large to medium predictive effect was shown for privacy concerns, whereas the privacy attitude only weakly predicts the information disclosure on social networks, for both identifiable and personal information.

4.3.1.3. Information disclosure on SNS (breadth) The breadth of information disclosure is defined as the range of topics that is posted on the SNS (Li et al., 2015). Analog to the general information disclosure on SNS, privacy concerns are also a good to moderate predictor for the breadth of information disclosure. A weak to moderate predictive effect was shown for gender (with females tending to disclose more broadly) and, to a lesser extent, for age, the degree pf activity and experience of the user on SNS. A marginal predictive effect was found for the number of posted blogs on the social network and the number of social network friends.

4.3.1.4. Information disclosure on SNS (depth) The depth of information disclosure refers to the sensitivity of the disclosed information (Li et al., 2015). Gender does not only predict the breadth, but also the depth of information disclosure on social networks on a small to moderate level, again with female users disclosing in more depth. Minor predictive effects have been shown for age, the number of social network friends, the user's degree of activity and experience on social networks, and the number of posted blogs on the SNS.

4.3.1.5. Information disclosure on SNS (less sensitive information) The disclosure of less sensitive information on SNS shows a similar picture regarding the predictive variables compared to the social network information disclosure breadth: Gender was shown to be a better – but still weak – predictor than user activeness and experience in social networks. On the other hand, age, along with the number of posted blogs and friends only marginally predict information disclosure.

4.3.1.6. Teenage information disclosure on social media Teenagers' disclosure of information about peer relationships on social media is best predicted by the intention to do so, whereas the willingness was found to be less important. They also tend to disclose more sensitive information if they also disclose basic information, for example their real name, birth date and school name. The results also suggest a moderate to small predictive value of social network complexity, which describes how diverse the network relationships of a

user are, for example whether s/he is friends with her/his parents, siblings, the extended family, school friends, other friends etc. The more complex the social networks, the more do teenagers tend to disclose personal and sensitive information. The size of the own social network (that is, number of social network friends) is also a weak to mediocre predictor for teenage information disclosure on social media, with teenagers disclosing more contact and insensitive information if they have a large number of social network friends. Somewhat smaller predictive value was found for social network usage frequency, age, gender (with males disclosing more contact information and females disclosing more peer relationship information), the direct intervention of parents in the information disclosure on social networks and the general trust in other people. Regarding the direct interaction with the SNS, teenagers disclose more information if they also set their profiles as private, if they have social network friends that do not go to school with them and also if they have strangers as friends on the social network. However, these relationships can also be considered as rather weak.

4.3.1.7. *Information disclosure towards a mobile app recommender* How much of their phone usage (context) and demographic data users disclose towards an app that recommends new apps based on the disclosed data is well to moderately predicted by their general collection concerns and weak to moderately by the extent of their mobile internet usage. However, users tend to disclose context data more easily than demographic data.

4.3.1.8. *Location disclosure on location-based social network application* Whether users disclose their location on location-based social network applications can at least be moderately predicted by their attitude towards such applications. Unlike for the prediction of general willingness to disclose data, the incentives gained through location disclosure serve only as weak predictor for the decision to actually disclose one's location on SNS apps.

4.3.1.9. *Sharing of profile information in a mobile app* Whether users share their personal profile in a mobile app with their friends or with every user of the app is somewhat predicted by their intent to disclose data in general.

4.3.2. *Usage of data sharing applications*
The included studies assessed the usage of a location sharing application as well as the usage of social network games.

4.3.2.1. *Usage of a location sharing application* Whether users decide to use a location sharing app or not is best predicted by the amount of benefits they can gain through the usage, with entertainment being twice as important as impression management (i.e., the ability of someone to control the impression of others toward him/her). Social influence and the intention to disclose data are small to mediocre and the competence-based and general trust in the location sharing application (LSA) network rather weak predictors for the usage decision.

4.3.2.2. *Usage of social network games* The usage intention was shown to be the only significant predictor for the actual usage of social network games.

4.3.3. *Privacy settings*
Privacy settings on SNS were assessed in general and specifically for teenagers.

4.3.3.1. *Privacy settings on SNS* How strict or lax users set their privacy settings in social networks is mainly predicted by their privacy intention, their privacy concerns (with a greater predictive effect for the Dutch social network Hyves than for the German network StudiVZ) as well as the perceived norms regarding what information should only be shared with friends. Stronger privacy concerns and more restrictive norms were related to stricter privacy settings, whereas the intention reflects the behavior insofar as users who want to distinguish their identity on Facebook are less identifiable (informational privacy), users who want to restrict access to their Facebook profile tend to do so (social privacy), users who want to have a less personal profile have one (psychological privacy) etc. A small to moderate predictive effect was shown for the tendency to use the internet for the purpose of impression management, the privacy attitude and high scores on the personality trait narcissism, i.e., the feeling of being a very special person. Impression management as usage purpose was related to less restrictive privacy settings, as were high values of narcissism. The effect of privacy attitude is similar to privacy intention, with users who think it is favorable to distinguish their identity on Facebook tend to be less identifiable etc.

4.3.3.2. *Teenage privacy settings on SNS* The privacy concerns of teenagers about their online data being collected by marketers weakly predicts their decision to implement privacy-setting strategies, such as deleting photo tags or intentionally posting false information about themselves. A weak association was also found between the implementation of these strategies and the teenagers' level of SNS use.

4.3.4. *Privacy protection behavior*
Again, in some studies privacy protective behaviors were assessed in general whereas others focused on protective behaviors of teenagers on SNS.

4.3.4.1. *Privacy-protective behaviors* Several variables were found to moderately to weakly predict the performance of privacy-protective behaviors: The years of experience someone has with using the internet, the perceived rewards one gets for data disclosure, privacy risk concerns and the tendency to believe that one is less likely to experience privacy infringements compared to younger users. Smaller predictive effects were found for internet usage, autonomy (not further specified), age (with younger users showing more privacy-protective behaviors), perceived personal risk, household income and gender, with males reporting higher levels of privacy-protective behavior.

4.3.4.2. *Teenage privacy protection on SNS* Teenagers are rather likely to remedy their disclosures on social networks if they also tend to interact with unknown others in a risky way on the corresponding SNS (rather strong predictor) and have privacy concerns (weak to mediocre predictor). Remedy of disclosure is further weakly predicted by female sex, tendency to disclose sensitive information, the performance

of advice-seeking behaviors, the participation of parents in direct intervention or active mediation as well as the frequent usage of SNS. Whether teenagers seek advice about their social network privacy behaviors is moderately to weakly predicted by their privacy concerns, their tendency to disclose sensitive information, and weakly by their age (with younger teenagers being more likely to seek advice) and gender (with female teenagers being more likely to seek advice) as well as the participation of their parents in direct interventions.

5. Discussion

The following section combines the identified privacy paradox explanation attempts, either derived from theoretical considerations or drawn from empirical studies. First, we identify the main predictors for privacy attitude, concerns, perceived risk, behavioral intention and behavior based on the empirical study results in Section 5.1. In Section 5.2, we discuss which implications these empirical study results hold for the theoretical privacy paradox explanation approaches. Section 5.4 deals with the practical implications and Section 5.5 with the limitations of this review. Finally, we draw some summarizing conclusions from this review in Section 5.6.

5.1. *Main predictors of privacy attitude, concerns, perceived risk, behavioral intention and behavior*

Although a multiplicity of significant predictor variables for privacy attitude, privacy concerns, perceived privacy risk, privacy behavioral intention and privacy behavior were investigated, unfortunately, no variable could be identified as a 'clear winner' for the prediction of the respective constructs. There are several possible explanations for this circumstance. First, many of the predictor variables were only investigated in a single study. However, some predictor variables were studied repeatedly, partially resulting in rather unequal effect sizes. The standardized path coefficients for the prediction of general intention to disclose information based on website trust, for example, ranged from 0.23 to 0.85. For the prediction of perceived privacy risk, the standardized path coefficients for prior experience with privacy infringement vary between 0.08 and 0.20. Furthermore, some of the authors relied on different definitions for the subordinate constructs attitude, concerns, perceived risk, behavioral intention and behavior or focused on very specific aspects of the respective construct, like teenage information disclosure on social media instead of general information disclosure. Finally, there are not only differences in the quality of the considered studies (see p. 46), but also in the characteristics of the considered sample (e.g., students vs. older participants, collectivistic vs. individualistic cultural background etc.). No inconsistencies should be caused by the employed study methodology, though, since all considered studies are surveys of an explanatory nature, i.e., aiming to find proposed causal relationships between variables.

In an attempt to still identify the most significant predictors for the different privacy aspects attitude, concerns, perceived risk, behavioral intention and behavior, all predictor variables with an effect size of at least 0.25 ($\beta \geq 0.25$) are listed in this section (Tables 34–37). In Figs. 2–5, the corresponding effect sizes found in the different studies are displayed.

5.1.1. *Privacy attitude, concerns and perceived risk*

Most of the variables with high predictive value indeed predict privacy attitude (or attitude towards specific products and technologies), instead of concerns or perceived risk. The list of very good predictors for attitude include trust towards the particular mobile website, information privacy concerns, computer anxiety, whether the user has granted permission for further data processing and the feeling of consumer alienation (i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices). Other good predictors are the user's self-esteem, whether s/he has experience in interacting with information technology, whether the respective data is only transferred further inside the data receiving corporation as well as the perceived security, playfulness and benefit regarding the application. Perceived career benefit is a mediocre predictor for social scientist's attitude towards sharing research data sets.

Among the most significant predictors for privacy concerns are situation-specific factors like the perceived risk or control, respectively, and the website's reputation. However, user-related factors like consumer alienation, self-esteem, computer anxiety and disposition to privacy also play a major role for the development of privacy concerns. How sensitive the particular data is, although still relevant, was found to be of less importance.

The results indicate that there are only mediocre predictors for perceived privacy risk, at least among the investigated variables. These comprise the level of trust in the recipient's ability to protect the provided data, the perceived protection through privacy regulations, the perceived relevance of the according information and the degree of personalization on the according website or application. Surprisingly, the study results suggest that privacy concerns and privacy risk awareness are also only moderately suited to predict perceived risk.

5.1.2. *Privacy related behavioral intention and willingness*

The benefits someone can gain through data disclosure represent important predictors for a user's behavioral intention as well as willingness to disclose data, either in a general way ('perceived benefit/value', 'perceived usefulness') or rather concrete ('liked targeted ads'). Regarding the user's individual characteristics, someone's need for consent and to what degree someone perceives oneself as similar to the subjective prototype of a user that discloses his/her data were found to be of most predictive power for intention and willingness to disclose data.

Although the identified effect sizes differ considerably across the considered studies, the trust a user has in a website significantly predicts his/her intention to share data with this website. This is in line with the significant predictive value of the user's privacy protection belief. Other important predictors for the behavioral intention are the level of (website, collection or general) privacy concerns, the perceived risk of data

Table 34 – Main predictor variables for privacy attitude, concerns and perceived risk.

Predictor variable	Outcome variable	Effect size (β)
Trust (TR)	Attitude towards location-based mobile website	0.79**
(Information) Privacy concerns (PC)	Attitude towards information practice	−0.70***
	Privacy attitude	0.25*** to 0.42***
	Perceived privacy risk	0.18*** to 0.34***
Computer anxiety (CANX)	Attitude towards information practice	−0.70***
	Privacy concerns (general)	0.37***
Perceived privacy risk (PPR)	Website privacy concerns	0.69**
	Privacy concerns (general)	0.44***
	Attitude towards location based social network apps	−0.37***
Permission granted (PG)	Attitude towards information practice	0.66***
Perceived control (PCO)	Context specific privacy concerns	−0.60**
Consumer alienation (CAL)	Attitude towards information practice	−0.61***
	Privacy concerns (general)	0.60***
Self-esteem (SE)	Privacy concerns (general)	−0.54***
	Attitude towards information practice	0.51***
Interaction with IT (IIT)	Attitude towards information practice	0.52***
Data transfer internally (DTI)	Attitude towards information practice	0.51***
Perceived security (PS)	Attitude towards social network games	0.50***
Perceived benefit (PB)	Attitude towards location-based social network apps	0.50***
Perceived playfulness (PP)	Attitude towards social network games	0.47***
Website reputation (WR)	Website privacy concerns	−0.20** to −0.45**
Disposition to privacy (DP)	Privacy concerns (general)	0.36***
	Website privacy concerns	0.20*
Perceived career benefit (PCB)	Social scientists' attitude towards data sharing	0.36***
Level of trust in the recipient's ability to protect data (LTAP)	Perceived privacy risk	−0.32***
Personalization (PER)	Perceived privacy risk	0.29**
Perceived relevance of information (PRI)	Perceived privacy risk	−0.28***
Perceived health information sensitivity (PHIS)	Health information privacy concern	0.28***
Perceived privacy regulatory protection (PPRP)	Perceived privacy risk	−0.25***
Privacy risk awareness (PRA)	Perceived privacy risk	0.25***

*p < .05.
**p < .01.
***p < .001.

Table 35 – Main predictor variables for privacy related behavioral intention and willingness.

Predictor variable	Outcome variable	Effect size (β)
Website trust (WT)	Intention to disclose information (general)	0.23** to 0.85***
	Intention to make Facebook data publicly accessible	0.28*** to 0.49***
Perceived benefit/ Perceived value (PB/PV)	Intention to disclose information on SNS	0.81***
	Willingness to disclose information	0.56** to 0.60**
Liked targeted ads (LTA)	Willingness to disclose information	0.59*** to 0.68***
Need for consent (NC)	Intention to make Facebook data publicly accessible	−0.14* to −0.58***
Retention period: indefinite (RPI)	Willingness to disclose information	−0.17* to −0.47***
Collection concerns (CC)	Intention to disclose data to an online retailer	−0.16* to −0.45***
Website privacy concern (WPC)	Intention to disclose information (general)	−0.43***
Perceived privacy risk (PPR)	Intention to disclose information (general)	−0.34* to −0.42***
Privacy concern (PC)	Willingness to disclose information	−0.25*** to −0.41***
	Intention to disclose information (general)	−0.15* to −0.27***
Willingness (WILL)	Intention to disclose information on SNS	0.34***
Perceived usefulness (PU)	Willingness to disclose information	0.33***
Usage scope: health site and Facebook (US:HF)	Willingness to disclose information	−0.33***
Usage scope: all sites (US:AS)	Willingness to disclose information	−0.30***
Attitude (ATT)	Intention to disclose information on SNS	0.32***
Prototype similarity (PS)	Willingness to disclose information about peer relationships on Facebook	0.32***
Privacy protection belief (PPB)	Intention to disclose information (general)	0.19* to 0.26***

*p < .05.
**p < .01.
***p < .001.

Table 36 – Main predictor variables for information disclosure behavior.

Predictor variable	Outcome variable	Effect size (β)
(Privacy) Intention (INT)	Information disclosure on SNS	0.65*** to 0.79***
	Teen information disclosure on social media	0.58***
	Usage of social network games	0.39*
General willingness to self-disclose (WILL)	Information disclosure (general)	0.59***
Collection concerns (CC)	Disclosure towards a mobile app recommender	0.22*** to 0.46***
Attitude towards location-based social network application (ATT)	Location disclosure on location based-social network application	0.43***
Privacy concerns (PC)	Information disclosure on SNS + Information disclosure on SNS (breadth)	−0.43***
Number of applications (NoA)	Information disclosure (general)	−0.35***
Benefits – entertainment (BEN-E)	Usage of a location sharing application	0.32***
Basic information disclosure (BID)	Teen information disclosure on social media	0.29***
Ads awareness (AA)	Information disclosure (general)	−0.28***
Social relevance (SR)	Information disclosure (general)	0.27***
Gender (GEN)	Information disclosure on SNS (depth)	−0.20** to −0.25**
Mobile internet usage (MIU)	Disclosure towards a mobile app recommender	0.15* to 0.25***

*p < .05.
**p < .01.
***p < .001.

Table 37 – Main predictor variables for protection behavior and privacy settings.

Predictor variable	Outcome variable	Effect size (β)
Risky interaction (RI)	Teenage privacy protection on SNS	0.44*** to 0.46***
Intention (INT)	Privacy settings on SNS	0.45***
Privacy (risk) concerns (PC)	Teenage privacy protection on SNS	0.10** to 0.36***
	Privacy settings on SNS	0.21** to 0.35**
	Privacy-protective behaviors	0.23***
Perceived norms regarding what to show only to friends (PN)	Privacy settings on SNS	0.31** to 0.33**
Years of internet experience (YIE)	Privacy-protective behaviors	0.21*** to 0.25***

**p < .01.
***p < .001.

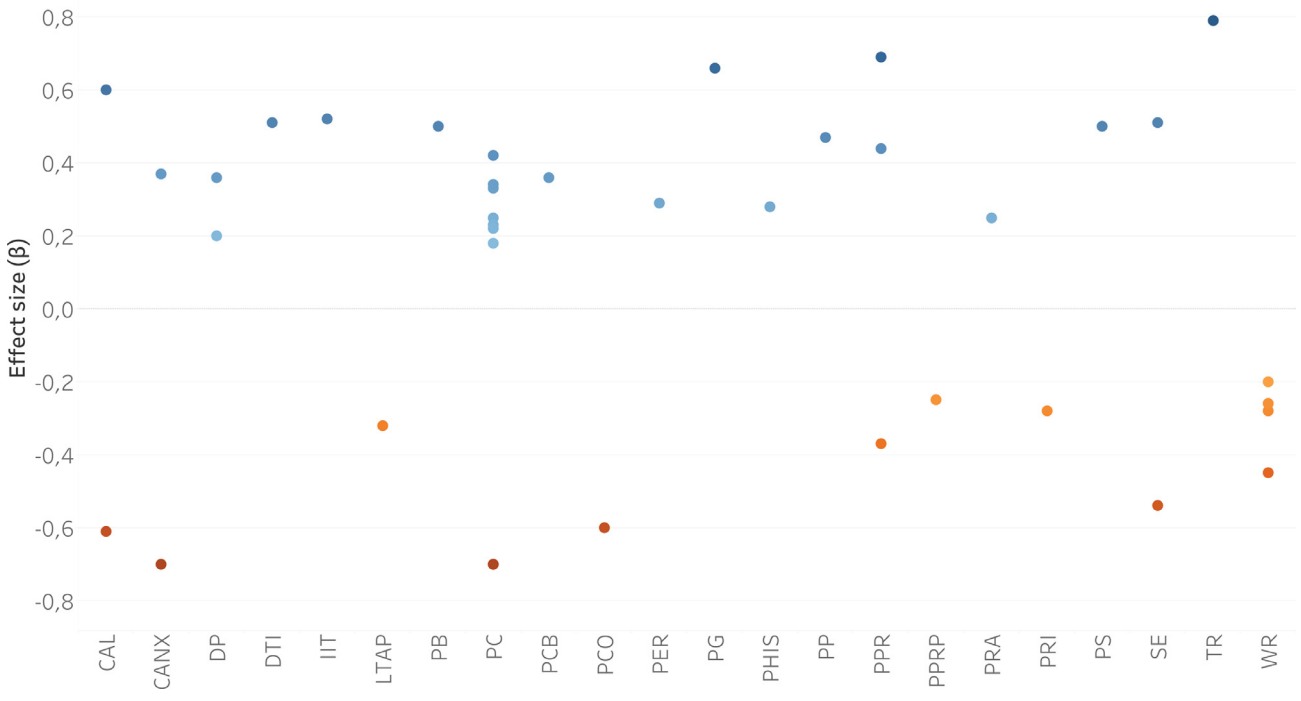


Fig. 2 – The effect sizes ≥ 0.25 reported in the included studies for privacy attitude, concerns and perceived risk.

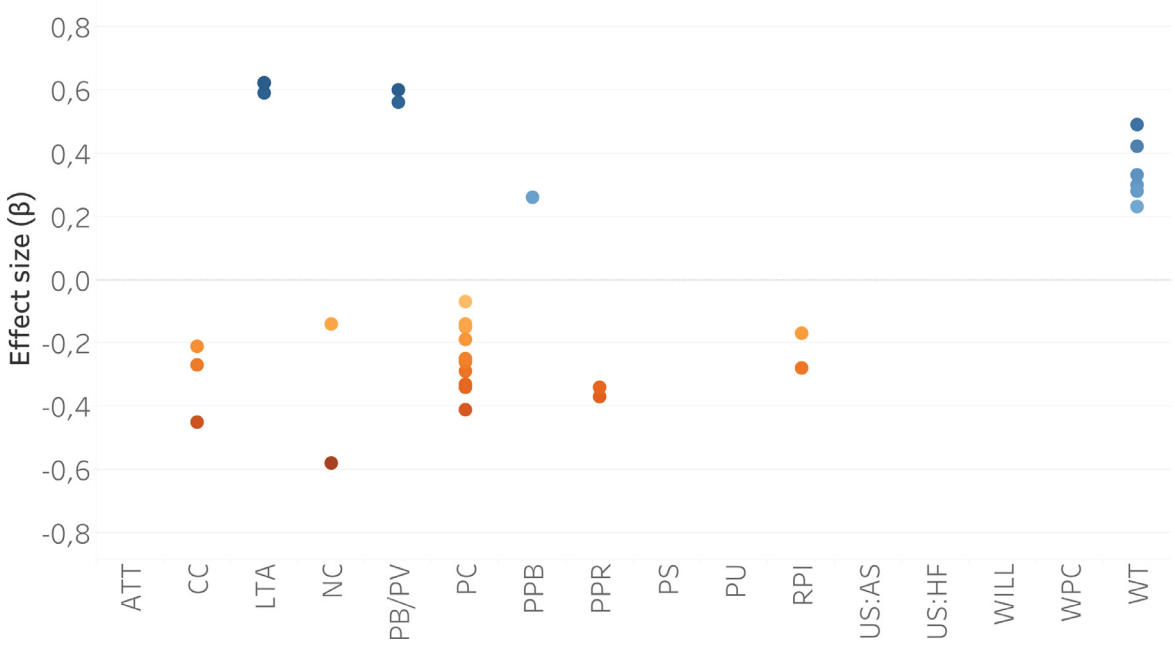


Fig. 3 – The effect sizes ≥ 0.25 reported in the included studies for privacy related behavioral intention and willingness.

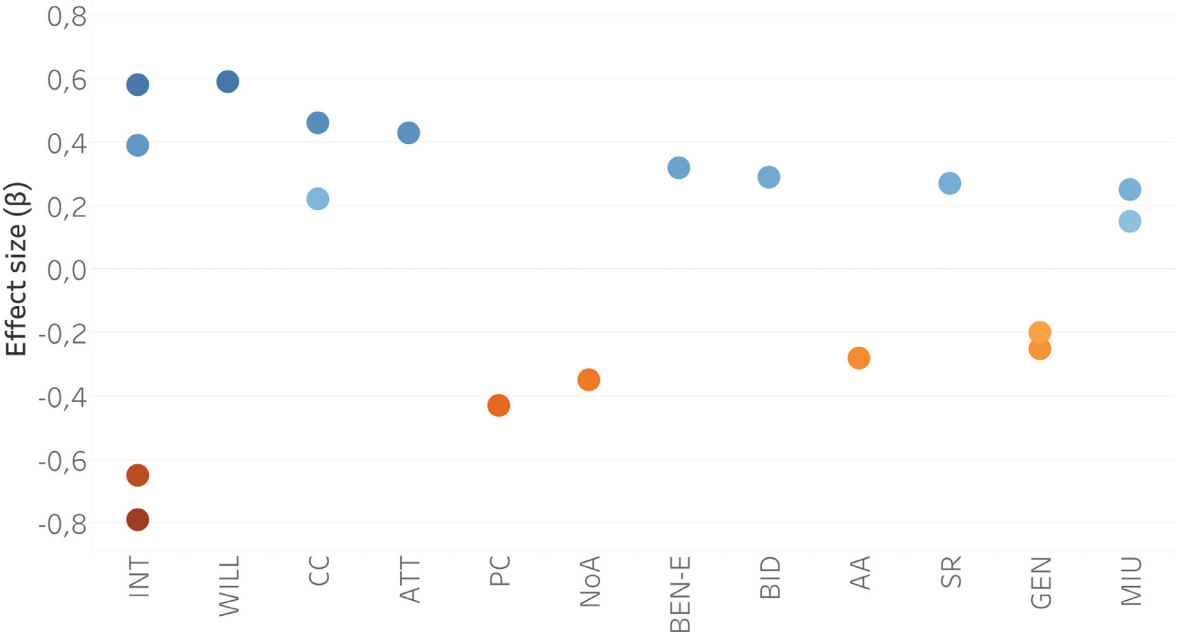


Fig. 4 – The effect sizes ≥ 0.25 reported in the included studies for information disclosure behavior.

disclosure, the general attitude towards data sharing and willingness to share data. Nonetheless, it is noteworthy that willingness to disclose data only predicts 34% of the variance in behavioral intention.

General privacy concerns were found to be an even better predictor for willingness to disclose data than for behavioral intention. Important situational factors for the willingness to disclose data are the usage scope of the respective website, along with the retention period of the disclosed data.

5.1.3. *Information disclosure behavior*

One of the most important predictors for actual data disclosure is the intention to disclose data, along with the general willingness to self-disclose. Concerns regarding data collection or privacy infringement were found to be of lesser, but still significant, importance for the prediction of disclosure behavior. Furthermore, other more or less privacy related behaviors like the number of used applications, the disclosure of basic information or the extend of mobile internet usage were found to predict disclosing behavior to some degree. Other sig-

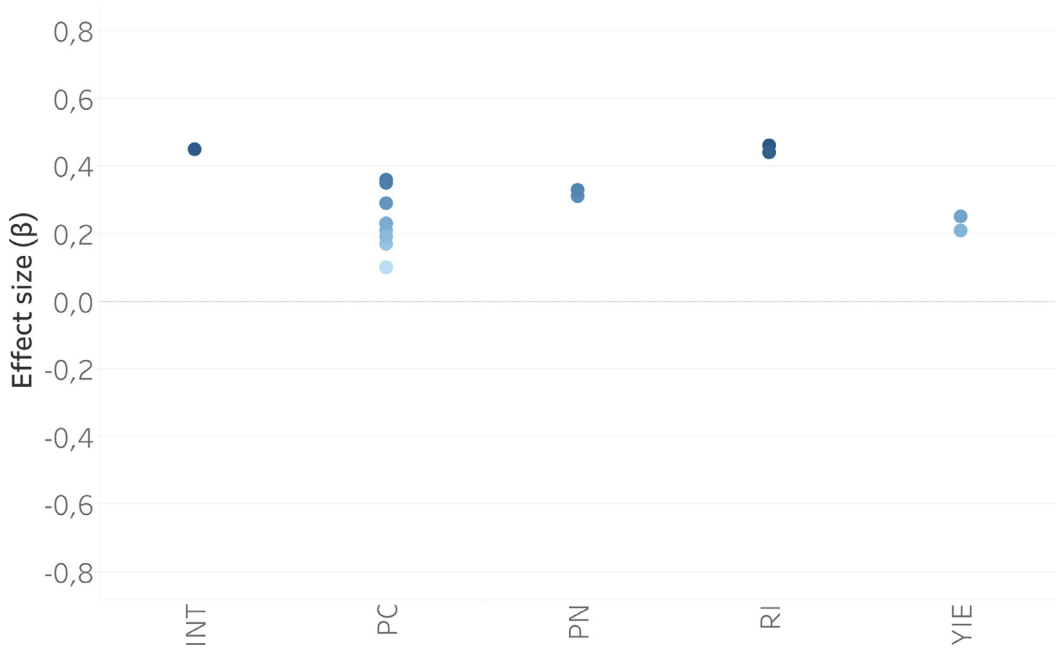


Fig. 5 – Main predictor variables for protection behavior and privacy settings.

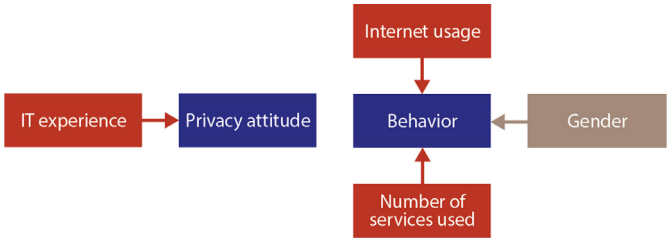


Fig. 6 – Relationship between main predictor variables and investigated outcome variables related to the user's experience and demographics.

nificant predictors for disclosing behavior are the user's attitude towards the receiving application, the perceived entertainment benefits that can be gained through disclosure, the user's general awareness of ads and the perceived relevance of the social web in the user's social environment. Information disclosure behavior was further shown to be the only outcome variable that can be somewhat predicted by a demographic variable, with female users being more likely to disclose their data.

5.1.4. *Protection behavior and privacy settings*

Whether a user shows protective behavior, including the management of privacy settings in social networks is best predicted by his/her participation in risky interactions and his/her behavioral intention. The perceived social norms concerning specific privacy settings, the experience someone has with using the internet and the expressed privacy concerns are of mediocre predictive value.

5.1.5. *Relationships between the main predictor variables*

The relationships between the main predictor variables and the investigated outcome variables privacy attitude, concerns, perceived risk, behavioral intention and behavior found in the included studies are displayed in Figs. 6–9. We categorized the main predictor variables and identified predictor variables that are related to the user's experience and demographics (Fig. 6), the user's cognition (Fig. 7), characteristics of the respective online service (Fig. 8), and the user's privacy perceptions and beliefs (Fig. 9).

5.2. *Predictor variables for future studies*

Some path analyses did not achieve sufficient statistical power (≥ .8) to allow for a reliable decision about the investigated predictor variables. These predictor variables are thus interesting candidates for future studies. Whereas those variables that were found to have a significant predictive value in spite of insufficient power are marked by an 'i.p.' in the results section, potential predictor variables which failed to provide significant predictions are displayed in Tables 38–41.

5.2.1. *Privacy attitude, concerns and perceived risk*

Table 38.

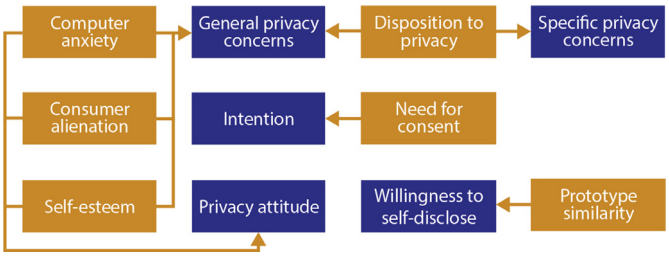


Fig. 7 – Relationship between main predictor variables and investigated outcome variables related to the user's cognition.

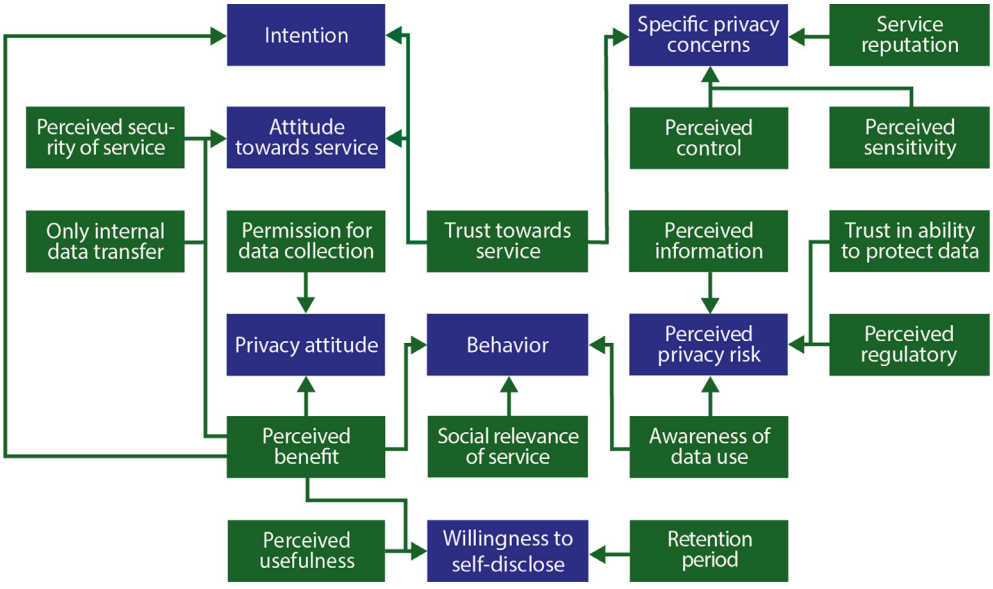


Fig. 8 – Relationship between main predictor variables and investigated outcome variables related to characteristics of the respective online service.

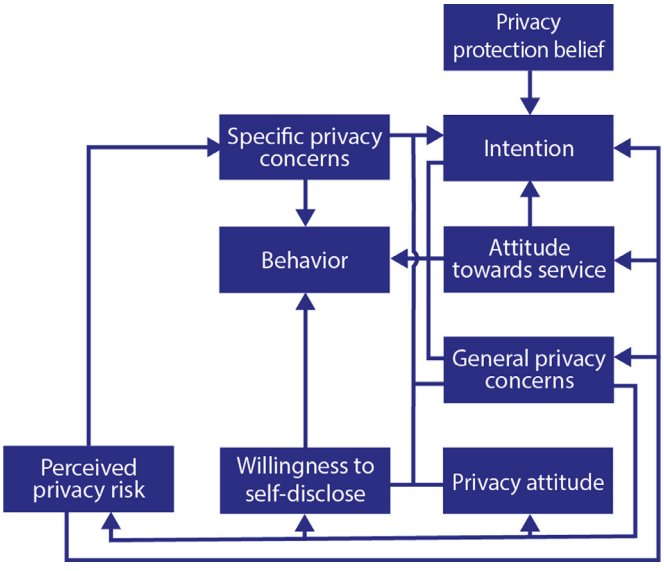


Fig. 9 – Relationship between main predictor variables and investigated outcome variables related to the user's privacy perceptions and beliefs.

Table 38 – Predictor variables for privacy attitude, concerns and perceived risk lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
SNS complexity			
Concern-centric model	Teenage privacy concerns on SNS	Jia et al. (2015)	588/ 6051
Risk-centric model			588/ 10,433
Age			
Concern-centric model	Teenage privacy concerns on SNS	Jia et al. (2015)	588/ 1,325,882
Risk-centric model			588/ 1,325,882
Gender			
Concern-centric model	Teenage privacy concerns on SNS	Jia et al. (2015)	588/ 11,430
Risk-centric model			588/ 15,453
Basic Information Disclosure			
For sensitive information	Teenage privacy concerns on SNS	Jia et al. (2015)	588/ 43,789
			588/ 52,994
Information sensitivity	Website specific privacy concerns	Xu et al. (2013)	171/ 20,468
Subjective norm	Website specific privacy concerns	Xu et al. (2013)	171/ 2241
Perceived enjoyment	Attitude towards Social network games	Shin and Shin (2011)	280/ 326
Perceived usefulness	Attitude towards social network games	Shin and Shin (2011)	280/ 192
Personalization			
For overt-based scenario	Perceived privacy risk	Xu et al. (2011)	278/ 1713
Previous privacy experience			
For overt-based scenario	Perceived privacy risk	Xu et al. (2011)	278/ 1257
General privacy concerns	Website specific privacy concerns	Li (2014a)	110/ 962
Internet experience	General privacy concerns	Li (2014a)	110/ 362
Gender	General privacy concerns	Li (2014a)	110/ 362
Age	General privacy concerns	Li (2014a)	110/ 15,451
Education	General privacy concerns	Li (2014a)	110/ 1713
Website familiarity			
For low reputation websites	Website specific privacy concerns	Li (2014)	110/ 143
Individual self-protection	Context specific privacy concerns	Xu et al. (2012)	178/ 1257
Government legislation	Context specific privacy concerns	Xu et al. (2012)	178/ 759
Age	Context specific privacy concerns	Xu et al. (2012)	178/ 61,827
Gender	Context specific privacy concerns	Xu et al. (2012)	178/ 15,451
Education	Context specific privacy concerns	Xu et al. (2012)	178/ 61,827
Desire for information control	Context specific privacy concerns	Xu et al. (2012)	178/ 962
Trust propensity	Context specific privacy concerns	Xu et al. (2012)	178/ 3860
Awareness of privacy statement	Perceived privacy risk	Li et al. (2011)	175/ 5344
Internet literacy			
For experienced shoppers	General privacy concerns	Liao et al. (2011)	259/ 614
Social awareness			
For experienced shoppers	General privacy concerns	Liao et al. (2011)	259/ 425
Education	Perceived privacy risk	Baek and Kim (2014)	2028/ 6865
Household income	Perceived privacy risk	Baek and Kim (2014)	2028/ 61,827
Liberal-conservative	Perceived privacy risk	Baek and Kim (2014)	2028/ 61,827
Internet use	Perceived privacy risk	Baek and Kim (2014)	2028/ 6865
Online knowledge	Perceived privacy risk	Baek and Kim (2014)	2028/ 61,827
Paternalisitic personality	Perceived privacy risk	Baek and Kim (2014)	2028/ 2469
Age	General privacy concerns	Abbas and Mesch (2015)	567/ 1038
Power disctance	General privacy concerns	Abbas and Mesch (2015)	567/ 1012
Uncertainty avoidance	General privacy concerns	Abbas and Mesch (2015)	567/ 386,412
Trust in technology	Perceived privacy risk	Miltgen et al. (2013)	326/ 1222
Level of trust in the recipient's willingness to protect data	Perceived privacy risk	Beldad et al. (2011)	208/ 507

5.2.2. *Privacy related behavioral intention and willingness*

Table 39.

5.2.3. *Information disclosure behavior*

Table 40.

5.2.4. *Protection behavior and privacy settings*

Table 41.

5.3. *Theoretical implications of the empirical study results*

Regarding the previously proposed explanations for the privacy paradox (see Section 3), some of the suggested variables were indeed strongly associated with the corresponding privacy constructs, whereas other variables were shown to be only weakly related to privacy attitude, concerns, perceived risk, behavioral intention or actual behavior.

Table 39 – Predictor variables for privacy related behavioral intention and willingness lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Coupon proneness			
For overt-based scenario	Willingness to disclose information	Xu et al. (2011)	278/ 3860
Trust in website	General intention to disclose information	Norberg et al. (2007)	68/ 9141
Negative affect			
For high security websites	General intention to disclose information	Wakefield (2013)	163/ 2197
For low security websites			138/ 51,097
Positive affect			
For low security websites	General intention to disclose information	Wakefield (2013)	138/ 1899
Privacy protection belief			
For high security websites	General intention to disclose information	Wakefield (2013)	138/ 298
Privacy concerns	General intention to disclose information	Li (2014a)	110/ 61,827
Disposition to privacy	General intention to disclose information	Li (2014a)	110/ 962
Age	Willingness to disclose information	Leon et al. (2013)	
	For demographic information		2912/ 386,412
	For location information		2912/ 96,604
Perceived privacy risk	Intention to disclose Information on SNS	Xu et al. (2013)	171/ 36,585
Information control	Intention to Disclose Information on SNS	Xu et al. (2013)	171/ 171.740

5.3.1. *Privacy calculus*

There definitely is some evidence for the privacy calculus model (Kokolakis, 2017), with possible benefits the user can gain through data disclosure being among the best predictors for disclosing intention as well as actual disclosure. At the same time, users do not seem to consider possible benefits when reflecting about their privacy concerns. This is in line with the privacy calculus model, which describes the weighting of costs and gains only within the decision process about actual behavior.

5.3.2. *Bounded rationality & decision biases*

Although there is no evidence for a strong relationship between the three privacy constructs attitude, behavioral intention and behavior and any of the variables describing a psychological bias (Acquisti and Grossklags, 2007; Kokolakis, 2017), at least optimism and affect were found to be mediocre predictors for protective behavior and behavioral intention, respectively.

5.3.3. *Lack of personal experience and protection knowledge*

Concerning technical knowledge and experience (Dienlin and Trepte, 2015; B2B International with Kaspersky Lab, 2015) computer anxiety was found to predict privacy attitude very well and privacy concerns to some degree, whereas actual experience (e.g., number of used applications, mobile internet usage, years of experience with using the internet) significantly predicts actual privacy behavior. Surprisingly, the study results suggest that prior experience with privacy infringements actually does not serve as a good predictor for privacy attitude, behavior or behavioral intention. However, it could be possible that the considered studies did not include enough participants who had actually experienced a serious infringement of their privacy in the past, leading to a lack of statistical power for that factor. Hence, further research is needed to investigate the potential influence of prior experiences with privacy infringement.

5.3.4. *Social influence*

Mainly behavior (disclosure and protection) was found to be predicted through social factors like the perceived social norm of what information should be only shared with friends and the social relevance of social networks. This is in line with the proposed influence of social factors (Kokolakis, 2017; Taddicken, 2014), on especially actual behavior, for behavior being the only variable that can actually be observed by the user's social environment.

5.3.5. *The risk and trust model*

There is only partial support for the risk and trust model (Flender and Müller, 2012; Miltgen et al., 2013): The perceived privacy risk is indeed one of the best predictors for privacy concerns, whereas the user's trust in the recipient's ability to protect his/her data serves as a rather mediocre predictor. Conversely, trust in a location-based mobile website was found to be an excellent predictor for the user's attitude towards that website. Additionally, trust is of major significance for the prediction of the behavioral intention, at least according to some of the study results. Perceived risk was also found to predict behavioral intention to some extent. However, neither risk nor trust were a significant predictor for actual privacy behavior, contradictory to the proposed model, which suggests trust to be a significant predictor for privacy behavior. The importance of trust for the prediction of the user's behavioral intention and attitude does not exactly fit to the proposed model either. Therefore, further research is needed to clarify the interplay of risk and trust on the one side and privacy attitude or concerns, behavioral intention and behavior on the other side.

5.3.6. *Illusion of control*

To what extend the user feels in control about the disclosure and processing of his/her personal data (Brandimarte et al., 2013) significantly predicts his/her privacy concerns, but there is no evidence for a significant relationship of perceived control and behavioral intention or behavior. However, only few of the considered studies investigated the influence of perceived

Table 40 – Predictor variables for information disclosure behavior lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Privacy concerns	General information disclosure	Taddicken (2014)	2739/ 17,483
Website specific privacy concerns	Basic information disclosure	Jia et al. (2015)	588/ 43,789
	For sensitive information		588/ 82,827
Ease of SNS privacy control	Basic information disclosure	Jia et al. (2015)	588/ 23,529
	For sensitive information		588/ 27,016
Age	Basic information disclosure	Jia et al. (2015)	
	For sensitive information		588/ 432,912
Gender	Basic information disclosure	Jia et al. (2015)	432,912
Trust in website	General information disclosure	Norberg et al. (2007)	68/ 51,097
Perceived privacy risk	General information disclosure	Norberg et al. (2007)	68/ 3049
Privacy concerns	Information disclosure	Dienlin and Trepte (2015)	
	For authentic first name		595/ 6865
	For authentic second name		595/ 1257
	For cell-phone number		595/ 15,451
	Political or religious views		595/ 1553
	Frequency of posts on SNSs		595/ 1713
Gender	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 759
	For personal information		588/ 21,387
Age	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 1772
	For contact information		588/ 2197
Parents' education	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 6034
	For personal information		588/ 3339
Parents' race	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 1604
	For contact information		588/ 1604
Hispanics	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 4766
Household income	Teenage information disclosure on social media	Xie and Kang (2015)	
	For contact information		588/ 42,936
SNS use frequency	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 813
	For contact information		588/ 2794
Network size/ Number of friends	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 653
Having SNS friends that do go to school with the participant	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 1772
	For contact information		588/ 31,546
Having SNS friends that do not go to school with the participant	Teenage information disclosure on social media	Xie and Kang (2015)	
	For insensitive information		588/ 893
	For contact information		588/ 7347
Having family members as SNS friends	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 1257
	For contact information		588/ 1459
Having strangers as SNS friends	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 31,546
Trust	Teenage information disclosure on social media	Xie and Kang (2015)	

(*continued on next page*)

Table 40 (*continued*)

Predictor variable	Outcome variable	Primary study	Actual N/required N
	For personal information		588/ 1967
Privacy settings	Teenage information disclosure on social media	Xie and Kang (2015)	
	For personal information		588/ 2039
Facilitating conditions	Location disclosure on location-based social network application	Koohikamali et al. (2015)	303/ 17,123
Information search	Usage of a location sharing application	Beldad and Citra Kusumadewi (2015)	655/ 1713
Information dissemination	Usage of a location sharing application	Beldad and Citra Kusumadewi (2015)	655/ 2469
Character-based trust in LSA	Usage of a location sharing application	Beldad and Citra Kusumadewi (2015)	655/ 6865
Privacy concerns	General information disclosure	Taddicken (2014)	2,739/ 17,483
Website specific privacy concerns	Basic information disclosure	Jia et al. (2015)	588/ 43,789
	For sensitive information		588/ 82,827
Ease of SNS Privacy control	Basic information disclosure	Jia et al. (2015)	588/ 23,529
	For sensitive information		588/ 27,016
Age	Basic information disclosure	Jia et al. (2015)	588/ 432,912
	For sensitive information		
Gender	Basic information disclosure	Jia et al. (2015)	432,912
Trust in website	General information disclosure	Norberg et al. (2007)	68/ 51,097

Table 41 – Predictor variables for protection behavior and privacy settings lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Education	Privacy-protective behaviors	Park (2015)	
	Social behavior		419/ 1066
Household income	Privacy-protective behaviors	Park (2015)	
	Technical behavior		419/ 1333
Marriage	Privacy-protective behaviors	Park (2015)	
	Technical behavior		419/ 1415
	Social behavior		419/ 5673
Autonomy	Privacy-protective behaviors	Park (2015)	
	Social behavior		419/ 3501

control, so the lack of empirical evidence could be probably caused by the lack of empirical studies in the first place.

5.3.7. *Quantum theory and the privacy paradox as methodological artefact*

There are also few studies dealing with quantum theory or the privacy paradox as methodological artefact, apart from the research introduced in Section 3. Again, further studies are needed to decide about the adequacy of the proposed models and explanations. However, the results implicate that researchers should indeed distinguish between privacy attitude and privacy concerns, as proposed by Dienlin and Trepte (2015).

5.4. *Practical implications*

Researchers and developers can build on the results to systematically construct privacy enhancing or privacy friendly technologies. Since the behavioral intention was found to be one of the main drivers for privacy protection behavior, a promising approach would be to focus on enhancing this behavioral intention to protect one's privacy. Behavioral intention, on the other hand, was found to be best predicted by service-specific characteristics and the user's privacy concerns or perceived risk, respectively. A first step would thus be to raise lay users' awareness of privacy issues, e.g., through privacy awareness campaigns or messages. A third factor for the user's privacy intention relates to social considerations. Another possible approach could therefore be to emphasize restrictive social privacy norms of peers and family members or focus on groups of users to collectively enhance their privacy behavior instead of individuals. However, the users' intention to protect their privacy can only result in successful protection behavior if they also know how to protect themselves. Hence, it is important to provide them with knowledge of and the ability to use protection solutions as well. This might be best achieved by addressing users with different levels of technical expertise separately, as the number of years someone has already interacted with the internet was also shown to be a valuable predictor of privacy protection behavior.

However, privacy researchers and developers should not only aim to implement factors related to privacy protective behavior. It would also be worthwhile to take a closer look at the factors that prevent privacy friendly behavior, for example whether the user strives for certain benefits or discloses data for a certain purpose like impression management. Privacy friendly alternatives need to provide the same core functionalities the users value on the original products (e.g., gained benefits and possibility for impression management) or only a small part of users will trade their familiar products for privacy friendly ones in the long run.

Further, privacy researchers can take the reported effect sizes into account when planning their study designs and exclude variables that have repeatedly shown to be negligible. They could, on the other hand, also comprise all significant variables in one model and conduct a comprehensive study of user privacy behavior. We are currently conducting a study which follows this approach. Last but not least, researchers are encouraged to further investigate the possible predictor variables which could not be confirmed or rejected due to lacking statistical power in the studies included in this review.

5.5. *Limitations*

Although a first step towards understanding the complex construct of privacy behavior and attitude, the present study suffers from several limitations. First, the literature search that forms the basis of this review was not exhaustive and thus presents only a first step towards understanding which variables are most relevant for the prediction of privacy attitude and behavior. Further systematic reviews are needed to gain a more comprehensive picture of the complex phenomenon 'user privacy'. Also, the underlying body of literature might suffer from publication bias, due to the general tendency in research to preferably publish positive or significant results, compared to negative or insignificant results. This should be kept in mind when interpreting the results or planning user studies on its basis. Furthermore, we focused on quantitative results drawn from survey studies using regression analysis and structural equation modeling, thereby omitting findings not only from qualitative research, but also from quantitative experimental studies which used other analyses methods, e.g., analysis of variance. It would be interesting to compare the findings from these research approaches with the present results. Last, we did not account for differences in the quality or representativeness of the receptive studies. Future reviews could for example weigh the particular effect sizes based on study quality.

6. Conclusion

Several possible explanations for the privacy paradox can be found in the literature. A closer look on the effect sizes of the variables predicting either privacy attitude, concerns, perceived risk, behavioral intention or behavior across different studies provides strong evidence for the privacy calculus model and the influence of social factors on privacy behavior. Further research is needed to evaluate the influence of prior experiences with privacy infringement and perceived control about the disclosure and processing of the disclosed data as well as the risk and trust model, quantum theory and the possible explanation of the privacy paradox as a methodological artefact. Demographic variables were only weak predictors of privacy attitude, behavioral intention or behavior. Only gender was found to predict privacy behavior to some degree, with female users disclosing more information.

Although there is a multiplicity of survey studies concerning user privacy in some way, it is difficult to draw overall conclusions, because in many cases the authors rely on slightly different constructs (e.g., privacy concerns, website privacy concerns, context specific privacy concerns). It is often not clear how these constructs relate to each other: For example, intention and willingness to disclose information could possibly refer to the same construct or describe two theoretically distinct concepts. Furthermore, several variables like consumer alienation and self-esteem were only investigated in a single study. It would therefore be beneficial for the privacy research community to agree on a shared definition of the relevant privacy constructs and further specify the relationship between these.

Acknowledgements

The research reported in this paper has been supported by the German Federal Ministry of Education and Research (BMBF) within MoPPa (KIS1DSD066). This work has also been cofunded by the DFG as part of project D.1 within the RTG 2050 "Privacy and Trust for Mobile Users".

Appendix. Quality assessment

Study	1	2	3	5	6	7	8	9	10	11	12	13	14	15	16	17
[71]	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[45]	Y	Y	N	Y	Y	N	Y	N	N	N	Y	N	NA	N	N	N
[62]	Y	Y	Y	Y	Y	N	Y	N	Y*	N	Y	N	NA	N	Y	Y**
[34]	Y	Y	N	Y	Y	N	Y*	N	Y*	N	Y	N	Y	NA	Y	Y
[59]	Y	Y	Y	Y	Y	N	Y	Y*	Y*	N	Y	Y	NA	N	Y	Y
[18]	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y
[64]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	NA	N	Y	Y
[38]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N
[39]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N
[72]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	Y	Y	Y
[37]	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y
[27]	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y*	N	Y	Y
[44]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
[41]	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[21]	Y	Y	Y	Y	Y	N	Y*	N	N	N	Y	Y	Y*	N	Y	Y
[40]	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
[28]	Y	Y	N	Y	Y	N	Y	Y	Y*	Y	Y	N	NA	N	Y	Y
[70]	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	NA	N	Y	Y
[68]	Y	Y	Y	Y	Y	N	Y*	N	N	N	Y	Y	Y*	N	Y	Y
[31]	Y	Y	NA	Y	Y	NA	Y	Y	NA	Y	N	NA	NA	N	Y	Y
[7]	Y	Y	Y	Y	Y	N	Y	Y*	Y	N	Y	Y	NA	N	Y	Y
[8]	Y	Y	N	Y	Y	N	Y	Y	Y*	Y	Y	N	NA	N	Y	Y
[51]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
[69]	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	Y*	N	Y	Y
[65]	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	N	NA	N	Y	Y
[46]	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	NA	N	Y	Y
[36]	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	NA	N	Y	Y
[74]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[1]	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	NA	N	Y	N
[33]	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[9]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[43]	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y
[11]	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	N	N	Y	Y
[10]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	NA	N	Y	Y
[74]	Y	Y	Y	Y	Y*	N	Y	N	Y	N	Y	N	NA	N	Y	N
[63]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	NA	N	Y	Y
[53]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[29]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y

Note: *fulfilled in part, **study 1 and 3: Y, study 2: N

Quality criterions

Sources:

Original form: Malhotra and Grover (1998), "An assessment of survey research in POM: from constructs to theory," *Journal of Operations Management*, Vol. 16 No. 4, pp. 407–425.

Clarification/comment: Sommestad et al. (2014), "Variables influencing information security policy compliance: A systematic review of quantitative studies", *Information Management & Computer Security*, Vol. 22, No. 1, pp. 42–75.

General

1. Is the unit of analysis clearly defined for the study?

Original form: a formal statement defining the unit of analysis was needed for a positive assessment on this attribute. Justification of why that unit of analysis was selected.

Clarification/comment: In the reviewed studies the unit of analysis was an employee in almost all cases. In all studies the unit of analysis was clearly defined.

2. Does the instrumentation consistently reflect that unit of analysis?

Original form: the items in the questionnaire would need to be at the same level of aggregation as the unit of analysis. For example, to ensure consistency, questions pertaining to overall business strategy must have strategic business unit as the unit of analysis. In contrast, manufacturing strategy related study could have the plant as the unit of analysis.

Clarification/comment: when the construct concerned a subjective property of an employee, which they often did, it was assessed if the questions were formulated this way. For example, a negative assessment was made if a respondent was asked "Does the security mechanisms work well?" for a construct called "perceived response efficacy" (because the question is not phrased as something perceived). All questions would need to be positively assessed.

3. Is the respondent(s) chosen appropriate for the research question?

Original form: the person most knowledgeable at the selected unit of analysis must be the preferred respondent. It would be inappropriate for instance, to survey plant employees on organizational constructs for a multi-plant organization.

Clarification/comment: in most cases the questions concerned an individual employee which made the respondent suitable. However, a negative assessment was made if arbitrary employees were asked question of objective nature which are outside of their expected competence, e.g., if a security policy is optimal.

Measurement error

5. Are multi-item variables used?

Original form: multiple items or questions would have to be used as opposed to a single item question to define a construct of interest. A positive assessment was made if both multi-item and single item variables were used in the study.

Clarification/comment: None.

6. Is content validity assessed?

Original form: content validity would need to be assessed through prior literature, or opinion of experts who are familiar with the given construct.

Clarification/comment: A negative assessment was made if the constructs was not discussed at all for the majority of the constructs.

7. Is field-based pretesting of measures performed?

Original form: a positive assessment was made only if the study formally stated the inclusion of this step in cleaning up the survey instrument and establishing its relevance.

Clarification/comment: studies that included a pre-test of pilot involving respondents somewhat representative to the population (e.g., students) received a positive assessment.

8. Is reliability assessed?

Original form: Cronbach's Alpha analysis or test–retest analysis would be needed for a positive assessment.

Clarification/comment: a positive assessment was made regardless if the reliability was assessed before (.e.g., in a pilot) or after data collection was made.

9. Is construct validity assessed?

Original form: construct validity (discriminant/convergent) analysis in the form of exploratory factor analysis, item-construct correlation, etc., would be needed for a positive assessment.

Clarification/comment: None.

10. Is pilot data used for purifying measures or are existing validated measures adapted?

Original form: a positive assessment was made if constructs and their associated items were evaluated on the basis of pretesting before the collection of actual data. Alternatively, constructs which were well defined and tested in prior studies could also be used.

Clarification/comment: the validity would need to be evaluated using a field-based pretesting (cf. item number 7). However, no formal/statistical evaluation was required.

11. Are confirmatory methods used?

Original form: confirmatory factor analysis (e.g., using LISREL) results would need to be reported to establish construct validity.

Clarification/comment: this should be a test made of the measurement instruments validity prior to its use and the test should confirm its correctness.

Sampling error

12. Is the sample frame defined and justified?

Original form: a discussion of sample frame was needed for a positive assessment.

Clarification/comment: the discussion would need to describe the sample frame to a level of detail that makes it possible to produce a similar sample. Since it is difficult to define the parameters that are needed to replicate the study (it depends on beliefs concerning extraneous variables) the criterion was applied leniently. At a minimum, however, it should be stated which country and type of organization that the sample frames includes and is not enough to explain who answered the questionnaire without detailing who was invited.

13. Is random sampling used from the sample frame?

Original form: sampling procedures (random or stratified) would need to be discussed for a positive assessment.

Clarification/comment: a positive assessment was also made if all samples within the sample frame were invited.

14. Is the response rate over 20%?

Original form: a formal reporting of response rate over 20% was needed for a positive assessment.

Clarification/comment: in case interest to participate in the study and answer the questionnaire was assessed before the final invitation was sent the response rate for those reporting interest was used.

15. Is non-response bias estimated?

Original form: a formal reporting of non-response bias testing was needed for a positive assessment.

Clarification/comment: None.

Internal validity error

16. Are attempts made to establish internal validity of the findings?

Original form: at the very minimum, a discussion of results with the objective of establishing cause and effect in relationships, elimination of alternative explanations, etc., was needed for a positive assessment. Statistical analysis for establishing internal validity (like structural equation modeling) was considered as desirable, but not critical.

Clarification/comment: in case the study confirmed all of the hypotheses it tested the motivation of these hypotheses was considered sufficient.

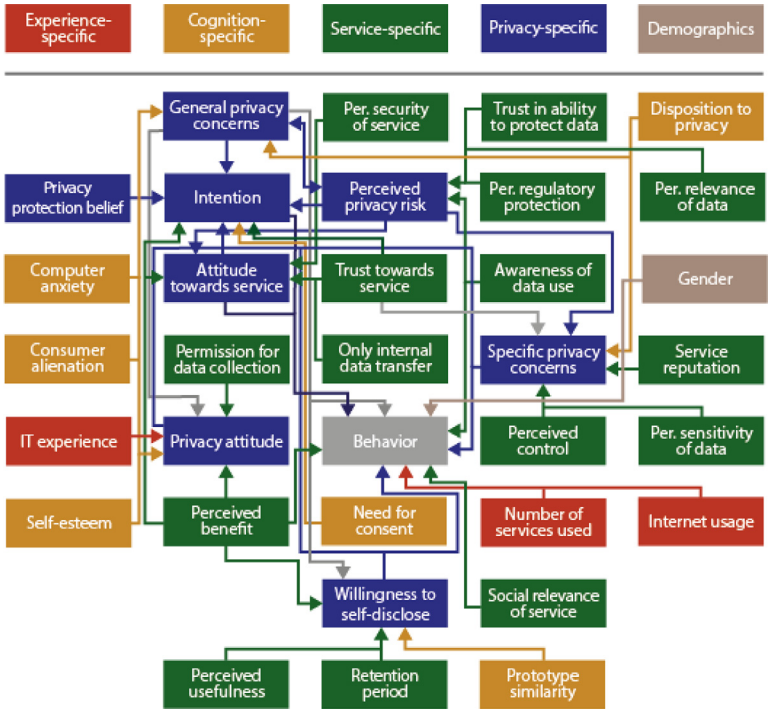
Statistical conclusion error

17. Is there sufficient statistical power to reduced statistical conclusion error?

Original form: at least a sample size of 100 and an item to sample size ratio of more than 5 were needed for a positive assessment.

Clarification/comment: None.

Relationships between the main predictor variables



REFERENCES

Abbas R, Mesch GS. Cultural values and Facebook use among Palestinian youth in Israel. Comput Hum Behav 2015;48:644–53. doi:10.1016/j.chb.2015.02.031.

Acquisti A, Grossklags J. Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. Proceedings of the second annual workshop on economics and information security (WEIS 2003), 2003.

Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur Priv 2005;3(1):26–33.

Acquisti A, Grossklags J. What can behavioral economics teach us about privacy?. In: Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, editors. Digital privacy: theory, technology, and practices. Boca Raton: Auerbach Publications; 2007. p. 363–77.

B2B International with Kaspersky Lab (2015). *Consumer security risks survey. From scared to aware: digital lives in 2015*. B2B International with Kaspersky Lab. https://press.kaspersky.com/files/2015/07/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_ENG.pdf/ Accessed 01 March 2017.

Baek YM. Solving the privacy paradox: a counter-argument experimental approach. Comput Hum Behav 2014;38:33–42. doi:10.1016/j.chb.2014.05.006.

Baek YM, Kim E-M. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns. Comput Hum Behav 2014;31:48–56.

Bansal G, Zahedi FM, Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 2010;49(2):138–50. doi:10.1016/j.dss.2010.01.010.

Becker L, Pousttchi K. Social networks: the role of users' privacy concerns. Proceedings of the fourteenth international conference on information integration and web-based applications & services – IIWAS '12; 2012. p. 187–95.

Beldad A, Citra Kusumadewi M. Here's my location, for your information: the impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. Comput Hum Behav 2015;49:102–10. doi:10.1016/j.chb.2015.02.047.

Beldad A, De Jong M, Steehouder M. I trust not therefore it must be risky: determinants of the perceived risks of disclosing personal data for E-government transactions. Comput Hum Behav 2011;27(6):2233–42. doi:10.1016/j.chb.2011.07.002.

Boyd D, Ellison NB. Social network sites: definition, history, and scholarship. J ComputMed Commun 2007;13(1).

Brandimarte, L., Acquisti, A., Loewenstein, G. (2009). Privacy concerns and information disclosure: an illusion of control hypothesis. In: Proceedings of the poster iConference.

Brandimarte L, Acquisti A, Loewenstein G. Misplaced confidences: privacy and the control paradox. Soc Psychol Personal Sci 2013;4(3):340–7. doi:10.1177/1948550612455931.

Cho H, Lee JS, Chung S. Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. Comput Hum Behav 2010;26(5):987–95.

Cohen J. Statistical power analysis for the behavioral sciences. 2nd ed. New York: Academic Press; 1988.

Deuker A. Privacy and identity management for life Privacy and identity 2009 IFIP Advances in information and communication technology, 320. In: Bezzi M, Duquenoy P, Fischer-Hübner S, Hansen M, Zhang G, editors. Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. Berlin, Heidelberg: Springer; 2011.

Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur J Soc Psychol 2015;45(3):285–97. doi:10.1002/ejsp.2049.

Downs A. An economic theory of democracy. New York: Harper & Brothers; 1957.

Faul F, Erdfelder E, Buchner A, Lang A-G. Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. Behav Res Methods 2009;41:1149–60.

Feng Y, Xie W. Teens' concern for privacy when using social networking sites: an analysis of socialization agents and relationships with privacy-protecting behaviors. Comput Hum Behav 2014;33:153–62. doi:10.1016/j.chb.2014.01.009.

Flender C, Müller G. Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Busemeyer JR, Dubois F, Lambert-Mogiliansky A, Melucci M, editors. Quantum interaction. Berlin Heidelberg: Springer; 2012. p. 148–59.

Gold RS, Brown MG. Explaining the effect of event valence on unrealistic optimism. Psychol Health Med 2009;14(3):262–72. doi:10.1080/13548500802241910.

Hull G. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics Inf Technol 2015;17(2):89–101. doi:10.1007/s10676-015-9363-z.

Ipsos & Centre for International Governance Innovation (2014). *83% of global internet users believe affordable access to the internet should be a basic human right*. Ipsos & Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf/ Accessed 01 March 2017.

Ipsos MORI (2014). *Global trends: personalisation* vs. *privacy*. Ipsos MORI. http://www.ipsosglobaltrends.com/personalisation-vs-privacy.html/ Accessed 01 March 2017.

Jia H, Wisniewski P, Rosson MB, Carroll JM. Risk-taking as a learning process for shaping teen's online information privacy behaviors. Proceedings of the computer supported cooperative work (CSCW) 2015:583–99. doi:10.1145/2675133.2675287.

Keith MJ, Thompson SC, Hale J, Lowry PB, Greer C. Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. Int J Hum Comput Stud 2013;71(12):1163–73. doi:10.1016/j.ijhcs.2013.08.016.

Kim Y, Adler M. Social scientists' data sharing behaviors: investigating the roles of individual motivations, institutional pressures, and data repositories. Int J Inf Manag 2015;35(4):408–18. doi:10.1016/j.ijinfomgt.2015.04.007.

Kitchenham, B. (2004). *Procedures for performing systematic reviews*. Keele University Technical Report TR/SE-0401. Keele University. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf/ Accessed 03 February 2017.

Knijnenburg BP, Kobsa A, Jin H. Dimensionality of information disclosure behavior. Int J Hum Comput Stud 2013;71(12):1144–62. doi:10.1016/j.ijhcs.2013.06.003.

Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput Secur 2017;64:122–34. doi:10.1016/j.cose.2015.07.002.

Koohikamali M, Gerhart N, Mousavizadeh M. Location disclosure on LB-SNAs: the role of incentives on sharing behavior. Decis Support Syst 2015;71:78–87. doi:10.1016/j.dss.2015.01.008.

Lee CH, Cranage DA. Personalisation-privacy paradox: the effects of personalisation and privacy assurance on customer responses to travel web sites. Tour Manag 2011;32(5):987–94. doi:10.1016/j.tourman.2010.08.011.

Lee N, Kwon O. A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. Expert Syst Appl 2015;42(5):2764–71. doi:10.1016/j.eswa.2014.11.031.

Leon PG, Ur B, Wang Y, Sleeper M, Balebako R, Shay R, et al. What matters to users? Factors that affect users' willingness to share information with online advertisers. Proceedings of the

ninth symposium on usable privacy and security – SOUPS '13, 2013.
Li H, Sarathy R, Xu H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decis Support Syst 2011;51(3):434–45. doi:10.1016/j.dss.2011.01.017.
Li Y. A multi-level model of individual information privacy beliefs. Electron Commerc Res Appl 2014a;13(1):32–44. doi:10.1016/j.elerap.2013.08.002.
Li Y. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decis Support Syst 2014b;57(1):343–54. doi:10.1016/j.dss.2013.09.018.
Li K, Lin Z, Wang X. An empirical analysis of users' privacy disclosure behaviors on social network sites. Inf Manag 2015;52(7):882–91. doi:10.1016/j.im.2015.07.006.
Liao C, Liu C-C, Chen K. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model. Electron Commerc Res Appl 2011;10(6):702–15. doi:10.1016/j.elerap.2011.07.003.
Malhotra M, Grover V. An assessment of survey research in POM: from constructs to theory. J Oper Manag 1998;16(4):407–25.
Miltgen CL, Popovič A, Oliveira T. Determinants of end-user acceptance of biometrics: integrating the "Big 3" of technology acceptance with privacy context. Decis Support Syst 2013;56(1):103–14. doi:10.1016/j.dss.2013.05.010.
Miltgen CL, Smith HJ. Exploring information privacy regulation, risks, trust, and behavior. Inf Manag 2015;52(6):741–59. doi:10.1016/j.im.2015.06.006.
Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. J Consum Affairs 2007;41(1):100–26. doi:10.1111/j.1745-6606.2006.00070.x.
Park YJ. Do men and women differ in privacy? Gendered privacy and (in)equality in the internet. Comput Hum Behav 2015;50:252–8. doi:10.1016/j.chb.2015.04.011.
Pew Research Center (2013). *Anonymity, privacy, and security online*. Pew Research Center. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ Accessed 01 March 2017.
Pew Research Center (2014). *Public perceptions of privacy and security in the post-snowden era*. Pew Research Center. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ Accessed 01 March 2017.
Plous S. The psychology of judgment and decision making. New York: McGraw-Hill Inc; 1993.
Rittenberg L, Trigarthen T. Principles of microeconomics. Washington, DC: Flat World Knowledge, Inc.; 2012.
Schwaig KS, Segars AH, Grover V, Fiedler KD. A model of consumers' perceptions of the invasion of information privacy. Inf Manag 2013;50(1):1–12. doi:10.1016/j.im.2012.11.002.
Schwarz N, Bless H, Strack F, Klumpp G, Rittenauer-Schatka H, Simons A. Ease of retrieval as information: another look at the availability heuristic. J Personal Social Psychol 1991;61:195–202.
Shin DH, Shin YJ. Why do people play social network games. Comput Hum Behav 2011;27(2):852–61. doi:10.1016/j.chb.2010.11.010.
Slovic P, Finucane M, Peters E, MacGregor GD. The affect heuristic. In: Gilovich T, Griffin WD, Kahneman D, editors. Heuristics and biases. Cambridge University Press; 2002. p. 397–420.
Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Q 2011;35(4):989–1016.
Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf Manag Comput Secur 2014;22(1):42–75.
Soper, D.S. (2018). A-priori sample size calculator for structural equation models [Software]. http://www.danielsoper.com/statcalc.
Symantec (2015). *State of privacy report 2015*. Symantec. http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf/ Accessed 01 March 2017.
Taddicken M. The "privacy paradox" in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. J Comput Mediat Commun 2014;19(2):248–73. doi:10.1111/jcc4.12052.
Tversky A, Kahneman D. Judgement under Uncertainty: Heuristics and Biases. Science 1974;185(4157):1124–31.
Tversky A, Kahneman D. The framing of decisions and the psychology of choice. Science 1981;211(4481):453–8. doi:10.1126/science.7455683.
Utz S, Kramer NC. The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. J Psychol Res Cybersp 2009;3(1).
Van Gool E, Van Ouytsel J, Ponnet K, Walrave M. To share or not to share? Adolescents' self-disclosure about peer relationships on facebook: an application of the prototype willingness model. Comput Hum Behav 2015;44:230–9. doi:10.1016/j.chb.2014.11.036.
Wakefield R. The influence of user affect in online information disclosure. J Strateg Inf Syst 2013;22(2):157–74. doi:10.1016/j.jsis.2013.01.003.
Wang N, Zhang B, Liu B, Jin H. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. Proceedings of the seventeenth international conference on human–computer interaction with mobile devices and services; 2015. p. 373–82.
Warshaw J, Matthews T, Whittaker S, Kau C, Bengualid M, Smith BA. Can an algorithm know the "real you"? Understanding people's reactions to hyper-personal analytics systems. Proceedings of the thirty-third annual ACM conference on human factors in computing systems; 2015. p. 797–806.
Wilson D, Valacich J. Unpacking the privacy paradox: irrational decision-making within the privacy calculus. Proceedings of the thirty-third international conference on information systems; 2012. p. 4152–62.
Wisniewski P, Jia H, Xu H, Rosson MB, Carroll JM. "Preventative" vs. "Reactive": How parental mediation influences teens' social media privacy behaviors. Comput Support Cooper Work Soc Comput 2015:302–16. doi:10.1145/2675133.2675293.
Xie W, Kang C. See you, see me: teenagers' self-disclosure and regret of posting on social network site. Comput Hum Behav 2015;52:398–407. doi:10.1016/j.chb.2015.05.059.
Xu F, Michael K, Chen X. Factors affecting privacy disclosure on social network sites: an integrated model. Electron Commerce Res 2013;13(2):151–68. doi:10.1007/s10660-013-9111-6.
Xu H, Luo X, Carroll JM, Rosson MB. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decis Support Syst 2011;51(1):42–52. doi:10.1016/j.dss.2010.11.017.
Xu H, Teo H, Tan BCY, Agarwal R. Research note – effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Inf Syst Res 2012;23(4):1342–63.
Zafeiropoulou AM, Millard DE, Webber C, O'Hara K. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions . Proceedings of the ACM Web Science Conference; 2013. p. 463–72.
Zhang B, Wu M, Kang H, Go E, Sundar SS. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. Proceedings of the thirty-second annual ACM conference on human factors in computing systems – CHI '14; 2014. p. 111–14.

Zhou T. Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors. Inf Syst Front 2015;17(2):413–22. doi:10.1007/s10796-013-9413-1.

Nina Gerber is a Ph.D. student at the Technische Universität Darmstadt in Germany. After she finished her studies of Psychology at the Technische Universität Darmstadt in 2015, she has been working as a doctoral researcher in the research group for Work and Engineering Psychology by Prof. Joachim Vogt at the Institute for Psychology in Darmstadt. In November 2017, she will start working as a doctoral researcher in the Secuso research group by Prof. Melanie Volkamer at the Department of Computer Sciences at the Technische Universität Darmstadt.

Her research interests relate to Human–Computer-Interaction, especially the privacy behavior of users and the field of usable security. Her publication list comprises research addressing the Privacy Paradox, user privacy behavior in social networks, acceptance and security perception of different authentication schemes, employee IT security behavior, and development and evaluation of usable tools which aim to support lay users to behave secure in the online context.

She is part of the Center for Research in Security and Privacy in Darmstadt and member of the German Usability Professionals Association. She has supervised several undergraduate research projects and theses, including research about mobile user privacy, the influence of perceived risk and trust on user privacy intention and behavior, psychological needs and goals relating to the use of data capturing online services, mental models of privacy and E2E encryption as well as perceived security and privacy concerns regarding the use of biometric authentication.