Telematics and Informatics 34 (2017) 1038–1058

Contents lists available at ScienceDirect

Telematics and Informatics

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

The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review

Susanne Barth [a,b,*], Menno D.T. de Jong [b]

[a] University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Services, Cybersecurity and Safety Research Group, PO Box 217, 7500 AE Enschede, The Netherlands

[b] University of Twente, Faculty of Behavioural, Management and Social Sciences, Department of Communication Science, PO Box 217, 7500 AE Enschede, The Netherlands

ARTICLE INFO

Article history:
Received 31 March 2017
Accepted 26 April 2017
Available online 28 April 2017

Keywords:
Information privacy
Privacy paradox
Decision-making
Privacy concerns
Risk
Benefit

ABSTRACT

Also known as the privacy paradox, recent research on online behavior has revealed discrepancies between user attitude and their actual behavior. More specifically: While users claim to be very concerned about their privacy, they nevertheless undertake very little to protect their personal data. This systematic literature review explores the different theories on the phenomenon known as the privacy paradox.

Drawing on a sample of 32 full papers that explore 35 theories in total, we determined that a user's decision-making process as it pertains to the willingness to divulge privacy information is generally driven by two considerations: (1) risk-benefit evaluation and (2) risk assessment deemed be none or negligible. By classifying in accordance with these two considerations, we have compiled a comprehensive model using all the variables mentioned in the discussed papers. The overall findings of the systematic literature review will investigate the nature of decision-making (rational vs. irrational) and the context in which the privacy paradox takes place, with a special focus on mobile computing. Furthermore, possible solutions and research limitation issues will be discussed.

Contents

* Corresponding author at: University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Services, Cybersecurity and Safety Research Group, PO Box 217, 7500 AE Enschede, The Netherlands.

E-mail addresses: s.barth@utwente.nl (S. Barth), m.d.t.dejong@utwente.nl (M.D.T. de Jong).

http://dx.doi.org/10.1016/j.tele.2017.04.013
0736-5853/

1. Introduction

The emergence of the Semantic Web has brought numerous opportunities with it, including an almost unlimited access to information, round-the-clock social networking connectivity and large scale data aggregation. It has grown to the extent that it now plays a part in the everyday lives of billions of people around the world. Simultaneously, the advent of big data and digital technologies has also raised serious privacy and security issues. Smith and Kollars (2015) called these digital developments 'the uncontrolled electronic panopticism' (p. 160). Fact is, the information being transformed between electronic devices equates to a form of unwitting user observation. When considering mobile applications and data 'leakage' in particular, recent literature argues that the consumer's choice to use mobile technologies is primarily driven by considerations of popularity, usability and the price of a given technology (Kelley et al., 2013; Kim et al., 2008) despite the potential risk of data misuse. At the same time however, research indicates that consumers are concerned about their privacy, including the ambiguous distribution of data and its use by third parties (Smith et al., 2011). This discrepancy between the expressed concern and the actual behavior of users is a phenomenon known as the privacy paradox: users claim to be very concerned about their privacy but do very little to protect their personal data. There are currently multiple theories explaining the privacy paradox. Some have explained this paradoxical behavior from a rational perspective by arguing that users weigh the cost-benefit ratio of online information disclosure both consciously and rationally (Simon, 1955). Others have questioned this rational view by arguing that individuals are bound in their rational decision-making by several cognitive biases, resulting in a pre-determinable cost-benefit calculation (Simon, 1982). Interestingly, both perspectives result in a risk-benefit calculation that ultimately chooses benefits over risks. In addition, an unbalanced decision-making process serves as the basis for a third perspective, where decision-making is based on prevalent benefits and as a result, no or negligible risk assessment takes place. Before introducing the present systematic literature review, the phenomenon of the privacy paradox will be discussed. After introducing the methodology, a review of the different theoretical approaches to the phenomenon will be presented. Lastly, the results will be discussed in terms of the nature of decision-making, the context within which the disclosure behavior takes places and solution-oriented implications.

1.1. The privacy paradox

The majority of research into the privacy paradox considers general internet activities with a focus on e-commerce and social networking activities in particular. Known as the privacy paradox, it is a documented fact that users have a tendency towards privacy-compromising behavior online which eventually results in a dichotomy between privacy attitudes and actual behavior (Acquisti, 2004; Barnes, 2006). A certain degree of risk perception implies greater knowledge of privacy protection strategies but appears an insufficient motivator to apply such strategies (Oomen and Leenes, 2008). Thus, while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behavior (Joinson et al., 2010; Pötzsch, 2009; Tsai et al., 2006). Furthermore, while an intention to limit data disclosure exists, actual disclosure often significantly exceeds intention (Norberg et al., 2007). Research into online service providers has shown that concrete privacy decisions and abstract risk awareness are not interchangeable. Privacy decisions do not change in line with modified preferences, which could explain the disparity between stated preferences for privacy and actual behavior (Flender and Müller, 2012). Although users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services (Acquisti and Grossklags, 2005; Sundar et al., 2013). In the context of users' social network activities, a similar pattern is observed. The utilization of various privacy protection strategies such as limiting wall post access, restricting photo tags and sending private messages instead of posting open content is designed to control to flow of information between friends and peers.

Implementing such strategies however, shows little concern for data collection by third parties in the background (Young and Quan-Haase, 2013). Privacy concerns should logically lead to restricted provision of information in social networks; however, the reverse effect can be observed as many users provide personal information seemingly without any hesitation (Hughes-Roberts, 2012; Manier and O'Brien Louch, 2010; Nagy and Pecho, 2009; Yoo et al., 2012). Looking at the provision of personal information in an app purchase process, Buck et al. (2014) found that information from ones' social group and the app store itself is more relevant than actual information about exploitation of personal data by third parties. Users are able to articulate their privacy needs but the actual decision to use (context-aware) applications does not align with their claims. Oetzel and Gonja (2011) go a step further, stating: privacy is not yet integrated into the social presentation of a smartphone and hence, will consequently lead to failed privacy awareness. Thus, supporting privacy awareness with suitable tools would allow meaningful decision-making by users and solve the conflicting interests between users and providers (Deuker, 2010). The previous discussion showed a variety of views on the emergence and existence of the privacy paradox. However, the cited literature discusses the discrepancy between privacy concerns and actual information disclosure from a practical point of view as it can be observed within the context of general internet activities, e-commerce, social networking sites and mobile applications. But what does the theory say about this phenomenon and why do users take so many risks? To our knowledge, there is not one unilaterally accepted theory used to explain the online behavior of users when it comes to information disclosure, nor is there a consensus on the mental processes users rely upon when deciding whether to disclose information or not. We did however, find a review of current research on the privacy paradox phenomenon (Kokolakis, 2017). The paper deals mainly with literature that either supports or challenges the existence of the privacy paradox under consideration of a number of theories, stressing the need for one theoretical model. The paper does not provide a full theoretical discussion of the phenomenon nor does the author offer any new ideas for solving the privacy paradox. Our systematic literature review on the other hand, attempts to develop an overarching theoretical framework, addressing the discrepancy between privacy concerns and actual online protective behavior through different theoretical lenses with a special focus on mobile applications.

2. Method

This paper presents a systematic literature review of all the studies that discuss the phenomenon of the so-called privacy paradox in the online environment. The main focus will be on mobile applications but as only nine studies addressing the subject could be ascertained via a literature search, the parameters in which the privacy paradox might be relevant were broadened to include social network sites, general online contexts, websites and e-commerce platforms.

An electronic database literature search was conducted in GoogleScholar, Scopus, IEEE, Web of Science and ACM. The keyword 'privacy paradox' was used as the primary broad search string. Papers were selected by their relevance as indicated by title or abstract and a subsequent examination of the full paper. Furthermore, a manual search of reference lists was conducted to identify additional papers that may have been missed by the electronic database search. Overall, only full, peer-reviewed papers, peer-reviewed conference papers and published book-chapters were included. Only the subject articles in which the phenomenon of privacy paradox was explicitly mentioned and discussed were considered eligible. Articles that dealt with privacy issues and concerns in general were not included. These searches resulted in an item set of 110 articles. In a second step, the articles were analyzed according to theories that had been applied to approach the phenomenon of the privacy paradox. Only articles that discussed the privacy paradox explicitly with the aid of a theory or theoretical concept were included in the final sample. Hence, articles that applied no theory at all or a theoretical approach or umbrella terms ("social capital", for instance) for discussing the phenomenon were excluded. Furthermore, articles discussing the personalization privacy paradox (a special subcategory of the privacy paradox) or solely providing a practical solution perspective, legal and ethical discussions/papers, research proposals and commentaries were excluded from the sample. This eventually resulted in a final sample of N = 32 full papers that accounted for 35 theories in total. In a third step, the articles were reviewed in detail with the aim of detecting clusters or divisions into which the different theories could be assigned. A pattern emerged, making a differentiation between rational and irrational approaches for paradoxical behavior. Furthermore, the majority of theories centered around a given cost-benefit calculation, with most favoring benefits over costs. An overview of all the clusters and the corresponding theories and articles discussed in the next section of this paper can be found in Table 1.

2.1. Approaches to the privacy paradox

When examining the nature and factors of decision-making, the applied theories (N = 35) were clustered into two main categories: (1) decision-making based on a risk-benefit calculation or (2) decision-making based on prevalent benefits and little to no risk assessment. The risk-benefit calculation category can be further divided into (1a) a largely rational calculation of risks and benefits whereas benefits outweigh risks, and (1b) a calculation process but risk assessment is biased and benefits are prevalent as a result. Both calculation processes ultimately lead to paradoxical behavior eventually. Category (1b) can be further divided into five different types of biases influencing the calculation process: (I) heuristics, (II) under- and/or overestimation of risks and benefits, (III) (immediate) gratifications, (IV) difference between judgments of risks and benefits, and (V) habit. The main category where no or marginal risk assessment only takes place accounts for three sub-categories:

Table 1
Overview of theories according to main categories and sub-clusters and corresponding articles.

Main category	Sub-cluster I	Sub-cluster II	Theory	Article(s)	Domain
Risk-Benefit Calculation	Risk-Benefit calculation guided by rationality	–	Rational Choice Theory of Human Behavior (Simon, 1955)	Hu and Ma (2010)	SNS
			Adaptive Cognition Theory of Social Network Participation (Hu and Ma, 2010)	Hu and Ma (2010)	SNS
			Privacy Calculus Theory (Culnan and Armstrong, 1999)	Chen and Chen (2015), Dinev and Hart, (2006), Kehr et al. (2014), Motiwalla et al. (2014), Pentina et al. (2016), Poikela et al. (2015) and Wilson and Valacich (2012)	e-commerce; mobile application; SNS; website
			Resource Exchange Theory (Donnenwerth and Foa, 1974; Foa, 1971)	Wilson and Valacich (2012)	e-commerce
			Expectancy Theory (Vroom, 1964)	Wilson and Valacich (2012)	e-commerce
			Rational Ignorance Theory (Downs, 1957)	Flender and Müller (2012)	Social web
			Theory of Reasoned Action/Theory of Planned Behavior (Ajzen and Fishbein, 1980; Ajzen, 1985)	Poikela et al. (2015)	e-commerce; SNS
			Dual Process Model of Cognition (System II) (Kahneman, 2003)	Phelan et al. (2016)	General online context
	Biased risk assessment within the risk-benefit calculation	Heuristics	Theory of Bounded Rationality (Simon, 1982)	Acquisti (2004), Acquisti and Grossklags (2005), Deuker (2010), Flender and Müller (2012), Jia et al. (2015), and Pötzsch (2009)	e-commerce; mobile application; SNS; social web
			Cognitive Heuristics (Tversky and Kahneman, 1975)	Gambino et al. (2016), Sundar et al. (2013), Wakefield (2013)	e-commerce, mobile websites
			Extension to the Privacy Calculus Theory (Culnan and Armstrong, 1999)	Kehr et al. (2015)	Mobile application
			Cues-filtered-out Theory (Sproull and Kiesler, 1986, 1991)	Pötzsch et al. (2010)	Web forums
			Feelings-as-Information Theory (Schwarz, 2011)	Kehr et al. (2014)	Website
			Structuration Theory (Giddens, 1984)	Zafeiropoulou et al. (2013)	Mobile application
			Communication Privacy Management Theory (Petronio, 1991, 2002)	Sundar et al. (2013)	e-commerce; SNS
		Under-/overestimation of risks and benefits	Optimistic Bias Theory (Irwin, 1953)	Acquisti (2004) and Flender and Müller (2012)	e-commerce; social web
			Theory of Under Insurance (Kunreuther, 1984)	Acquisti (2004)	e-commerce
			Third-Person Effect Theory (Davison, 1983)	Debatin et al. (2009)	SNS
		(Immediate) gratifications	Immediate Gratifications (O'Donoghue and Rabin, 2001)	Deuker (2010), Flender and Müller (2012), Acquisti (2004) and Wilson and Valacich (2012)	e-commerce; mobile application; Social web
			Self-Control Bias (Loewenstein, 1999)	Acquisti (2004), Acquisti and Grossklags (2005)	e-commerce
			Hyperbolic Discounting Theory (Laibson, 1997)	Acquisti (2004), Acquisti and Grossklags (2005), Flender and Müller (2012), Hughes-Roberts (2013) and Wilson and Valacich (2012)	e-commerce; SNS; social web
			Theory of Cognitive Absorption (Agarwal et al., 1997)	Alashoor and Baskerville (2015)	SNS
			Uses and Gratification Theory (Blumler and Katz, 1974; Katz et al., 1974)	Debatin et al. (2009) and Quinn (2016)	Mobile websites; SNS

(*continued on next page*)

Table 1 (*continued*)

Main category	Sub-cluster I	Sub-cluster II	Theory	Article(s)	Domain
		Difference between the judgements of risks and benefits	Prospect Theory (Kahneman and Tversky, 1979)	Hughes-Roberts (2013)	Privacy policies; SNS; website
			Quantum Theory (Based on Busemeyer et al., 2006)	Flender and Müller (2012)	e-commerce
		Habit	Theory of Ritualized Media Use (Rubin, 1984)	Debatin et al. (2009)	SNS
Little to no risk assessment	Value of desired goal outweighs risk assessment	–	Privacy Regulation Theory (Altman, 1975)	Shklovski et al. (2014)	SNS; social web
			Conformity and Peer group pressure (Crutchfield, 1955)	Flender and Müller (2012)	Social web
			Duality of Gemeinschaft und Gesellschaft (Tönnies, 2012)	Lutz and Strathoff (2011)	SNS
			Extended Two-Component Model of Self-Presentation Online (based on Leary and Kowalski, 1990)	Krämer and Haferkamp (2011)	SNS
	Privacy valuation failed	–	Public Value Theory (Meynhardt, 2009)	Lutz and Strathoff (2011)	SNS
			Social Representation Perspective (Moscovici, 1984; Abric, 1996)	Oetzel and Gonja (2011)	SN, Google and smartphone
	Knowledge deficiency due to incomplete information	–	Theory of Incomplete Information (Harsanyi, 1967)	Acquisti (2004), Acquisti and Grossklags (2005), Buck et al. (2014), Deuker (2010) and Flender and Müller (2012)	e-commerce; mobile application; Social web
			Dual Process Model of Cognition (System I) (Kahneman, 2003)	Phelan et al. (2016)	General online context
			Symbolic Interactionism (Blumer, 1986)	Young and Quan-Haase (2013)	SNS

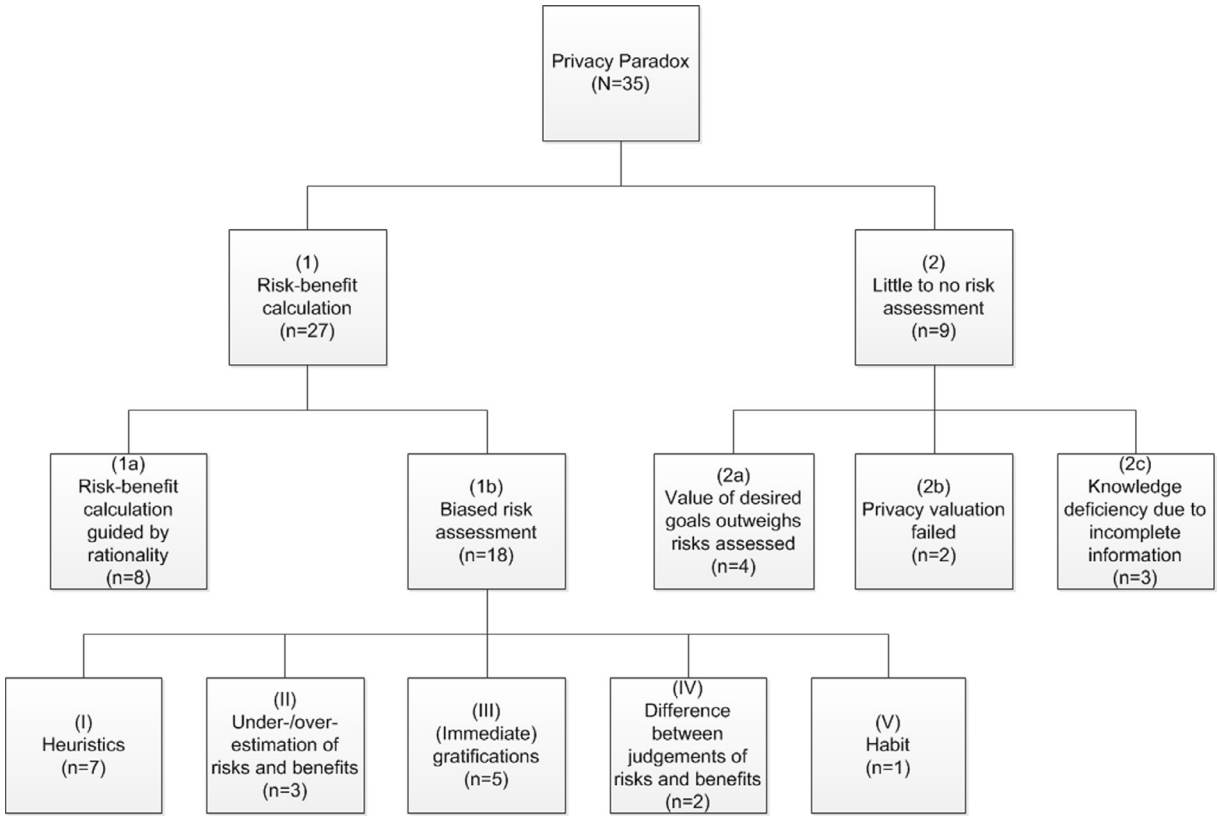

Fig. 1. Overview of categorization theories according to nature of decision making.

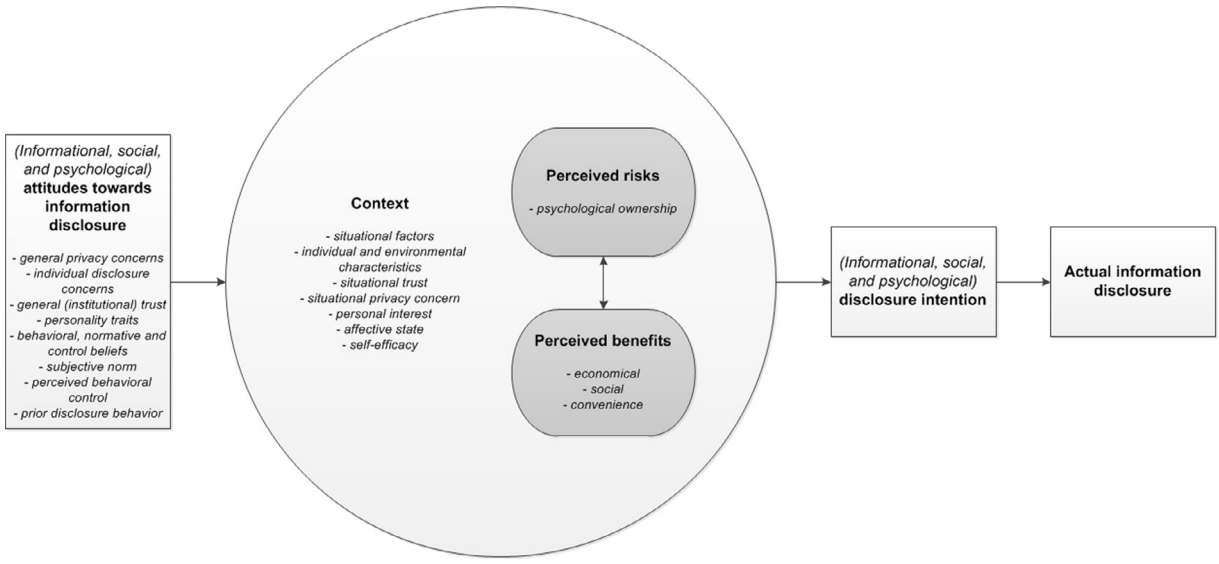

Fig. 2. Overview of variables that play a role in the risk-benefit calculation guided by rationality.

(2a) value of desired goals outweighs risks assessed. Additionally, this process is largely determined by in- and out-group considerations, (2b) the privacy valuation failed, and (2c) a knowledge deficiency eventuates as a result of incomplete information. The latter sub-category is also part of the bounded rationality approach but because it is deemed a failed risk assessment due to incomplete information, it was assigned to the second main category. In the following paragraph, the mentioned

categories will be discussed. For an overview of the categorization of the various theories, please see Fig. 1. A comprehensive description of the theories can be found in Appendix 1.

3. Risk-benefit calculation guiding decision-making processes

Some of the studies claim that rational processes account for this paradoxical behavior, as decisions are carefully considered by way of conscious-analytic, profit-loss calculations. In other words: users consciously weigh the disadvantages of privacy disclosure against the perceived benefits. It would seem that users consciously resolve discrepancies between the willingness to obtain and possess something (such as downloading an app) and the simultaneous difficulties that arise in terms of unknown threats or risks (such as potential data usage by third parties). In other cases, the risk-benefit assessment is not completely rationally calculated, rather subject to and influenced by factors such as time constraints, immediate gratification or optimistic bias. Quite often, users are not consciously aware of such a bias and as a consequence, choose benefits while ignoring accompanied risks.

3.1. Risk-benefit calculation guided by rationality

Risk-benefit calculation plays a major role in the context of information privacy, known as the freedom to decide with whom, how and to what extent personal data is shared (Li et al., 2010). The cognitive style of decision-making during risk-benefit calculations is both analytical and conscious and can be described as 'logical, cause and effect, rule-based, hierarchical, sequential, process-oriented, slower to implement but quicker to change, high effort, oriented toward delayed action, conscious, and experienced actively with the individual aware of and in control of the process' (p. 57, Novak and Hoffman, 2008). During information exchange, negative consequences are rationally weighed against goals and possible outcomes, aiming to maximize benefits and minimize the risks of information disclosure (Keith et al., 2013; Li, 2012; Vroom, 1964). Hence, intention and actual behavior are positively influenced by expected benefits (e.g. using an app) but also negatively affected by associated costs (e.g. possible data usage by third parties) (Culnan and Armstrong, 1999). Following, the different theories applied to the decision-making processes within the privacy calculation will be discussed. A comprehensive overview of all the variables that were mentioned in the following theories that play a role in the risk-benefit calculation is presented in Fig. 2.

According to *Rational Choice Theory of Human Behavior* (Simon, 1955) decisions are always reasonable and logical in order to gain the greatest benefit or satisfaction in line with an individuals' perceived self-interest. In decision-making, individuals seek to maximize utility and minimize risk through rational calculus in response to both internal and external constraints. When dealing with social media, users base their decision-making as it pertains to information disclosure on perceived benefits (e.g. networking with friends and acquaintances) and perceived risks (e.g. privacy and identity theft, image damage). Building on this rational view of decision-making, Hu and Ma (2010) propose the *Adaptive Cognition Theory of Social Network Participation*. Here, user participation in online social networks can be assigned to three phases: initial use, exploratory use and managed use. The progression from one phase to the next results from understanding the benefits and risks associated, as well as the adaptation of activities and controls. The final phase can be described as an equilibrium of benefits and risk awareness formed by a continuous process of risk-benefit calculation. Quite often, the perceived benefits outweigh the perceived risks, which eventually leads to the neglecting of privacy concerns that often results in the disclosure of information in exchange for social or economic benefit (*Privacy Calculus Theory;* Culnan and Armstrong, 1999). Within this calculation, economic benefits, personalization or convenience and social benefit tend to negate the downside of perceived risks (Wilson and Valacich, 2012). Individuals tend to concentrate on actual benefits rather than on previously stated concerns and calculated future risks with regard to issues such as location tracking by service providers via location-based mobile applications (Poikela et al., 2015). Moreover, an interdependency between the risk and benefit calculus exists as benefit valuations guide risk perception even if there is no relation in reality. Although users of social networks are confident they have taken adequate steps to control the flow of their private information (e.g. limiting profile visibility), this does not necessarily represent a significant decrease in the disclosure of personal information. This suggests that self-efficacy in privacy management on social networking sites can outweigh privacy concerns especially for those with low prior privacy concerns (Chen and Chen, 2015). Furthermore, the cumulative effects of internet trust and personal internet interests can outweigh privacy risk perception to point that it eventually leads to the disclosure of personal information as it pertains to e-commerce transactions for example (Dinev and Hart, 2006). Pentina et al. (2016) added the Big Five personality factors and the influence of cross-cultural differences to the privacy calculus model. Extraversion and agreeableness increased perceived benefits from the use of mobile applications, regardless of the cultural environment. The satisfaction of informational and social needs led to the continued use of mobile applications despite the knowledge personal information might well be compromised. Privacy concerns did not have any influence on the adoption and use of mobile applications. Even more, situational privacy calculus influences privacy disclosure as pre-existing attitudes (e.g. privacy concerns) may be fully overridden by situational factors such as the benefits associated with using a particular app) (Kehr et al., 2014). Prior information disclosure behavior is generally more indicative of privacy valuation traits or individual privacy concerns. Fundamentalists for example (those highly concerned about data sharing with third parties and unwilling to place ongoing trust in particular organizations) expressed higher privacy valuation than those with a more pragmatic stance (concerned about data-sharing practices but

willing to engage in privacy calculus activities), or unconcerned individuals (willing to share data, also with third parties without significant privacy concerns) (Motiwalla et al., 2014). In exchange for other resources such as money, services, time, status and love, people are willing to provide personal resources, including those in the form of personal information (*Resource Exchange Theory;* Donnenwerth and Foa, 1974; Foa, 1971). In such instances, personalization, convenience, economic benefits and social advantages will suppress the perception of risks while over-emphasizing the perceived benefits of privacy disclosure (Wilson and Valacich, 2012). Based on a subjective belief system, an individual chooses a certain behavior over another because of the expected outcome of maximizing benefits while minimizing costs (*Expectancy Theory*; Vroom, 1964). Here, the decision-making process is based on three beliefs: (1) valence (emotional attitude towards a particular outcome and the allure of receiving a reward); (2) expectancy (self-confidence to do s.th.); and (3) instrumentality (perception of the probability of gaining reward). As such, the conscious choice of an individual to ignore a certain piece of information is again based on a cost-benefit calculation, especially those where the informative effort (costs) are considered disproportionate to the perceived potential benefits (*Rational Ignorance Theory*; Downs, 1957). For instance, users may consider the cost of reading complex privacy policies in their entirety (e.g. loss of time or cognitive effort) outweighs the dangers, deciding that the benefits of using a service outweighs any potential privacy abuse concerns (Flender and Müller, 2012). Taking the intentional perspective of a given rational behavior into account, the *Theory of Reasoned Action* (Ajzen and Fishbein, 1980) states that an individual's behavioral intention depends on the attitude towards a certain behavior and the subjective norms. The stronger the intention, the more likely it is that a person will engage in a certain behavior. The *Theory of Planned Behavior* (*TPB*) (Ajzen, 1985) takes this a step further as behavioral intention is influenced by existing attitudes about desired outcomes, social norms and the evaluation of the risk-benefit of that outcome (perceived behavioral control). The stronger such attitudes, perceived control and the compliance with social norms are, the more likely it is that an individual will engage in a certain behavior. Actual control may be the missing variable that could explain the discrepancy between intention and behavior. The technological context of mobile apps adds various factors to the privacy calculus that are beyond the user's control such as near continuous tracking (Poikela et al., 2015). According to *Dual Process Model of Cognition* (Kahneman, 2003), decision-making is based on two systems. System 1 is fast and intuitive, whereas System II is rational and responsible for reasoning (resulting in legitimate concerns, for example). Intense intuitive concern may be overruled (but not reduced) by less intense concerns resulting from conscious consideration. Thus, privacy concerns are considered but most individuals are unable to address them adequately (Phelan et al., 2016). The previously discussed theories show that the decision process as it pertains to information disclosure is guided by rational cost-benefit calculations where benefits outweigh risks. However, the majority of the analyzed studies showed a markedly different tendency as the theories to explain the privacy paradox can be characterized by the non-rational processes of decision-making. Here, the risk assessment within the risk-benefit calculation is biased by internal or external forces.

3.2. Biased risk assessment within the risk-benefit calculation

Contrary to a risk-benefit calculation guided by rationality, decision making can also be influenced by different kinds of biases such as time constraints, time inconsistency, immediate gratification and optimistic bias. These biases are often non-conscious but play a major part in the eventual decision-making. Furthermore, bounded rationality also has an influence on

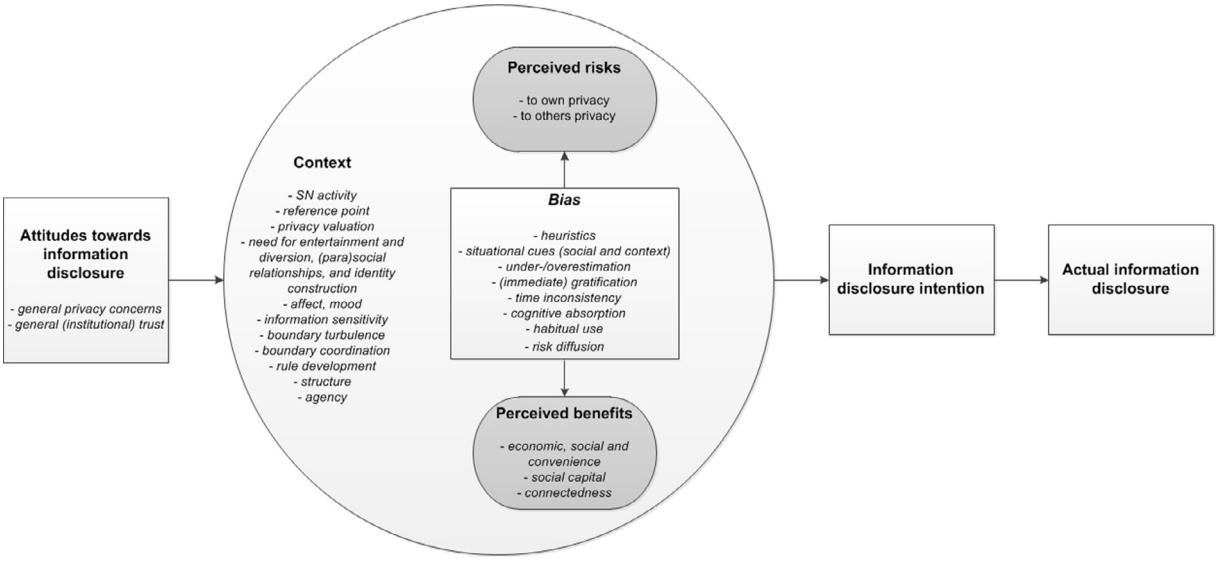

Fig. 3. Overview of variables that play a role in the biased risk assessment within in the risk-benefit calculation.

the decision-making process. Too many options, unpredictable consequences, uncertainties or cognitive limitations eventually lead to subconscious biases in the calculation process. Hence, a decision is usually rapidly derived without an orderly subsequent analysis of the situation. As such, it cannot be verified according to process or grounds for judgment, but is instead based on experience (formal knowledge or beliefs) or a confidence in virtue. The experiential processes are 'associative, emotional, low effort, rapid to implement but slow to change, parallel, immediate, outcome-oriented, holistic, preconscious and experienced passively with the process opaque to the individual' (p. 57, Novak and Hoffman, 2008). Following, the different theories of biased risk assessment within privacy calculation will be discussed. A comprehensive overview of all the variables that were mentioned in the theories that play a role in biased risk-benefit calculation is presented in Fig. 3.

3.2.1. Heuristics

Quite often, individuals are unwilling to access and process all of the information necessary to make informed decisions on issues affecting privacy due to perceived or actual cognitive limitations, choosing rather to satisfy themselves with subpar solutions. Individuals constantly try to rationally maximize benefits but decision-making can only be rational within the limits of cognitive ability and available time (*Theory of Bounded Rationality;* Simon, 1982). Hence, the objectively irrational decision-making of the privacy paradox can be explained by an individual's cognitive limitations as they pertain to accessing and processing all relevant information which could well lead to a biased perception of privacy risks. A user's ability to access all the relevant information is bounded by nature, leading to a situation where the risks are deemed to be outweighed by benefits (Deuker, 2010). However, from their subjective point of view, the decision process may well appear rational (Flender and Müller, 2012). Even users with privacy concerns prove extremely reluctant to take the necessary actions to become informed, even when the information to protect ones' privacy is made readily available (Acquisti and Grossklags, 2005). Information disclosure translates to a loss of control over that information and individuals find themselves in an information asymmetry which can be overcome through rational assessment. However, the factors that may play a role in that cognitive process are very difficult to aggregate, calculate and compare, requiring high cognitive involvement. As a result, the costs of adequate risk assessment can be perceived as unacceptably high leading individuals to rely on simple heuristics (Acquisti, 2004). In the context of social networking sites, teenagers in particular operate under bounded rationality and risk assessment takes place according to personal experiences pertaining to privacy invasion and not hypothetically in advance (Jia et al., 2015). Even if people theoretically have all of the necessary privacy-relevant information, they are unable to make proper sense of all of the information. This leads to the application of simplified mental models that are often favor the benefits (Pötzsch, 2009). Mental short-cuts allow individuals to come to decisions quickly while suppressing any urge to think about the next action (*Cognitive Heuristics*; Tversky and Kahneman, 1975). However, heuristics can lead to biases and an approach that has been successful in the past is no guarantee that it will prove suitable in another situation. Furthermore, heuristics hinder individuals from developing new ideas and alternative solutions. In their study of online privacy behaviors, Gambino et al. (2016) found a total of four positive heuristics (gatekeeping -, safety net -, bubble – and ephemerality heuristic) and four negative heuristics (fuzzy-boundary -, intrusiveness -, uncertainty – and mobility heuristic) that promote or inhibit information disclosure behaviors and possibly lead to the privacy paradox. In general, website cues that trigger affect heuristics (positive feelings about the website for instance) have a direct effect on the trust and faith that eventually leads to online information disclosure (Wakefield, 2013). Also Sundar et al. (2013) found that privacy disclosure behavior in an online context is determined heuristically rather than systematically, which leads to a positive attitude towards information disclosure. In reference to cognitive heuristics and mental shortcuts, Kehr et al. (2015) concluded that the privacy paradox may result from misleading situational cues which bias cognitive valuation processes (e.g. affective thinking) and the prevalence of situation-specific considerations as compared to generic attitudes (*Extension to the Privacy Calculus Theory*). Eventually, privacy disclosure intention is determined by situational cues even if dispositional attitudes regarding privacy behavior are different to intention. Hence, privacy decisions are driven by situation-specific privacy assessment, general dispositions (i.e. general privacy concerns, institutional trust) and affect-based heuristics (quite often unconscious processes). *Cues-Filtered-Out Theory* (Sproull and Kiesler, 1986, 1991) implies that individuals disclose more personal data in computer-mediated communication settings compared to face-to-face settings due to the absence of social and contextual cues leading to disclosure of information online despite general privacy concerns (Pötzsch et al., 2010). When considering emotional factors during decision-making processes, individuals rely upon their feelings (mood, meta-cognition, emotion and body sensation), which generally leads to accurate responses but not always (*Feeling-as-Information Theory*; Schwarz, 2011). For instance, being in a good mood lets people evaluate targets or situations as more positive than they may be. Furthermore, judgments are based on feelings of ease or difficulty, as situation or targets that are easy to process are evaluated as more likely to be of less risk and more valuable. Being in a positive mood positively influences privacy protection attitude, whereas being in a negative mood increases risk perception (Kehr et al., 2014). Considering interpersonal relationships, social life is more than individual acts, yet it is determined by social forces such as traditions, institutions and moral codes. Social structures determine human behavior but can also be altered as a result of perception, ignorance or replacement. Therefore, behavior is a balance between social structures and agency (the ability to act according to free will). The structure is achieved through a dynamic process (structure forms the basis for decision-making but is at the same time the outcome of it) *(Structuration Theory;* Giddens, 1984). While making privacy decisions with regard to the usage of mobile applications, people are constrained by structures (e.g. privacy requirements as a standard) which implies that they are unable to act entirely according to their free will (e.g. having general privacy concerns). This eventually leads to the negotiation of privacy by weighing costs against benefits. However, users are expected to accept certain requirements if they want to install and use a certain

app. This eventually results in a contradiction between stated privacy attitudes and actual behavior to the extent that sharing personal information becomes perceived as normal in social life (Zafeiropoulou et al., 2013). Likewise, decisions on what information to reveal and which to keep private are central to the *Communication Privacy Management Theory* (Petronio, 1991, 2002). Publication or retention is associated with particular risks and benefits. This process is guided by the subjective privacy boundaries that individuals have (as determined by an iterative process of rule development, boundary coordination and boundary turbulence), boundaries that are continually reshaped, depending on situation, context and communication partner(s). In this regard, rule development is assessed as a function of the nature of a given network (e.g. a network that is made of strong ties requires more information disclosure and therefore higher levels of privacy), whereby boundary coordination is tested by means of communication violation expectancy (e.g. if boundaries are violated, an individual might adjust their privacy settings in order to regain privacy). Hence, privacy decision-making is based on developed rules that depend on the perception of risks and benefits. However, this seems only be true for perceived privacy concerns and not for actual disclosure behavior, resulting in a 'heat of the moment' (p. 811) paradoxical behavior (Sundar et al., 2013).

3.2.2. Under- and/or overestimation of risks and benefits

Individuals tend to underestimate their own risk of privacy invasion while overestimating the chances that others will experience adverse events. This eventually leads to a belief that their own privacy is not at risk, a situation that can in turn eventually result in enhanced risk exposure (Acquisti, 2004; Flender and Müller, 2012). Furthermore, this lower risk perception might result in a laxer precautionary stance (*Optimistic Bias Theory;* Irwin, 1953). The tendency toward a reluctance to engage in privacy protection behavior against low probability but high impact/consequences events due to biased perception (event is less threatening than it actually is), underestimation of probability (as a consequence of little or no experience with the threat in question), unawareness of the threat or the costs of engagement are considered as too high is also discussed in the *Theory of Under Insurance* (Kunreuther, 1984). The underestimation of future risks may lead to a tendency to underinsure oneself against these risks (Acquisti, 2004).

Likewise, according to *Third-Person Effect Theory* (Davison, 1983), individuals tend to overestimate the effect of media on others while underestimating the influence on themselves. As a result, individuals usually do not demonstrate the intended behavior as a response to the message. In this regard, the negative effects of information disclosure in social networks are mostly ascribed to others while they consider themselves the beneficiaries of positive effects only (e.g. building and maintaining relationships) (Debatin et al., 2009). Although many users of social networks possess considerable privacy setting knowledge, they do not protect their private information properly as the perceived benefits outweigh any potential risks associated with information disclosure.

3.2.3. (Immediate) gratifications

In some cases, individuals encounter self-control problems as immediate gratification prompts atypical behavior which may be negative over the long term (*Immediate Gratifications*; O'Donoghue and Rabin, 2001; *Self-Control Bias*; Loewenstein, 1999). If there is choice, individuals usually choose a small benefit in the short term over a larger benefit in the longer term. If all choices are available over the long term, greater benefits will be chosen, even if these will occur later than smaller benefits (*Hyperbolic Discounting Theory*; Laibson, 1997). Individuals might have general privacy concerns; however this will not influence information disclosure behavior in the spur of the moment. Situational cues mitigate potential risks in the distant future and emphasize immediate benefits as users exhibit a tendency to favor immediate rewards on the short term at the expense of future risks due to a lack of self-discipline (e.g. using a search engine and getting a result immediately). This immediate gratification outweighs eventual privacy concerns resulting in poor risk protection by neglecting privacy protection technology even though they might encounter privacy violations in the future. Thus, individuals tend to heavily discount the low probability of high future risks (e.g. identity theft), resulting in a preference for almost instantaneous benefits (Acquisti, 2004; Acquisti and Grossklags, 2005; Deuker, 2010; Flender and Müller, 2012; Hughes-Roberts, 2013). During online transactions for example, users disclose private information in return for small benefits, even if their general privacy concerns are contrary to this behavior (Wilson and Valacich, 2012). In their study on information disclosure on social network sites, Alashoor and Baskerville (2015) found that *cognitive absorption* (Agarwal et al., 1997; Agarwal and Karahanna, 2000) during social networking activity can overrule privacy-related thinking as illustrated in the privacy calculus. The extensive use of social networking sites and the associated intrinsic rewards from that engagement can eventually lead to a flow state from being highly engrossed in such activities. This in turn can result in the kind of inappropriate behavior as it pertains to information disclosure that can lead to serious disadvantageous consequences affecting both career and private life. Looking at the motivation perspective (*Uses and Gratification Theory*; Blumler and Katz, 1974; Katz et al., 1974), media use is actively executed in order to achieve and satisfy certain goals and needs along the dimensions of diversion and entertainment, building and maintaining relationships and identity construction. This assumes that individuals recognize their needs and how to satisfy them. Participation in an online social networks offers gratification among all three dimensions of goals and needs which eventually outweighs possibly privacy concerns, even when perceived privacy violations occur (Debatin et al., 2009).

3.2.4. Difference between the judgments of risks and benefits

According to *Prospect Theory* (Kahneman and Tversky, 1979), decision-making processes take place in two stages. During the editing stage, expected outcomes are ordered according to the basis of heuristics by setting a reference point. During the

evaluation stage, outcomes below the reference point are considered losses and better outcomes as gains. However, individuals do not process information rationally. They value gains and losses differently as decisions are usually based on perceived gains rather than losses, with losses being judged more harshly than gains that might otherwise be judged equal. Hence, interaction with others via social networks (gain) can lead to privacy risk depreciation (loss) (Hughes-Roberts, 2013).

Making use of *Quantum Theory* (based on Busemeyer et al., 2006), Flender and Müller (2012) suggest that the choice between high and low privacy valuation and data disclosure and concealment are two incompatible types of preferences and an exchange of information between both cannot take place. Additionally, preferences are not predetermined but altered at the time an actual decision is made. Furthermore, privacy valuation and the associated privacy threats/risks are abstract concepts and data disclosure refers to concrete benefits. This explains why concrete benefits might often dominate abstract risks.

3.2.5. Habit

Repetitive behavioral patterns are addressed in the *Theory of Ritualized Media Use* (Rubin, 1984). (Social) media not only serves to satisfy information demands or entertainment needs, but can also be seen as a habit that's integrated into daily routines. Such routines form a part of temporary structures and social rituals. Debatin et al. (2009) conclude that the use of social networking sites is ritualistic and strongly integrated into people's everyday lives by means of creating social capital and connectedness through a broad network (which would not be possible in an offline context) so that these benefits outweigh privacy concerns and prevent engagement in privacy protection behavior, even in cases of direct privacy violations. Quinn (2016) found that habit (habit was identified as one out of nine uses and gratifications) probably inhibits engagement in privacy management tools on social networks, despite increased experience with social networking, which eventually leads to a disconnection between privacy concerns and behaviors.

3.3. Little to no risk assessment

There are certain situations in which individuals possess little to no privacy-related information whatsoever, such as those where goal obtainment nullifies all other considerations, or circumstances involving users that are unconcerned with privacy protection. Such situations result in significantly prevalent (perceived) benefits accompanied by negligible to no risk consideration. A complete risk-benefit calculation cannot take place under such circumstances and benefits are used as the sole reference point. Following, the different theories applied to the one-sided decision-making processes will be discussed. A comprehensive overview of all the variables that were mentioned in the following theories is presented in Fig. 4.

3.3.1. Value of desired goal outweighs risk assessment

Privacy can be described as a dynamic process of regulating interaction with others. In this process, in-group and out-group considerations play a major role. Thus, based on internal states and external conditions, individuals determine their acceptable degree of openness. Privacy regulation should be enforced at an optimal level (an equilibrium between the desired level of privacy and the actual level). Here, trust plays an important role in the interaction regulation process which is defined by the self-imposed boundary (around a person) which in turn is determined by self-disclosure and a dyadic

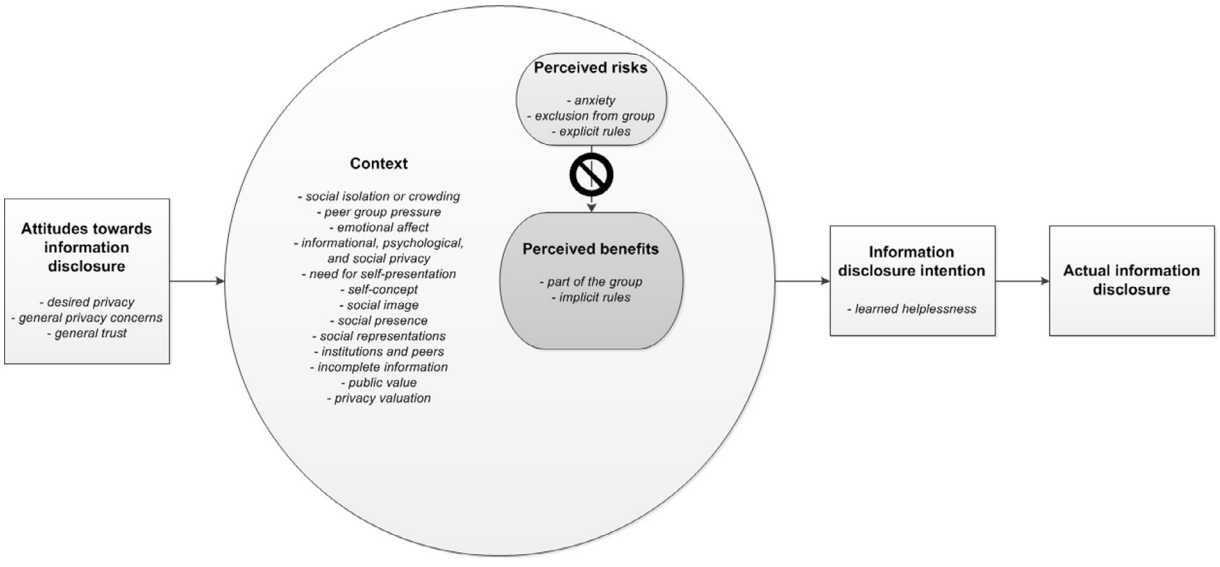

Fig. 4. Overview of variables that play a role in the decision making process with no to little risk assessment.

boundary (ensures the discloser's data security in the case of violation) (*Privacy Regulation Theory*; Altman, 1975). According to Shklovski et al. (2014) repeated invasion of privacy boundaries can lead to a state of resignation (learned helplessness). People do accept privacy policies by app developers despite privacy concerns for the mere reason of having access to the app (mobile apps usually act according to an all-or-nothing principle that implies that total acceptance of the privacy policy is inherent to use of the app) and because users are resigned to the fact that they possess little power to change the situation anyway. It would seem that the suppression of negative feelings as they pertain to the information sharing behaviors of some apps is simply part of the 'cost of doing business' – that is, the price one has to pay to use the app. An individual's attitudes and behavior are influenced by others (especially by close or important friends). Individuals feel indirectly pressured to adapt their own behavior to achieve conformity with the admired peer group. Peer group pressure can result in either positive or negative reactions (*Conformity and Peer group pressure;* Crutchfield, 1955). In their study on online service providers, Flender and Müller (2012) found that peer group pressure negatively influences the privacy decision process. In order to be a group member, individuals neglect privacy concerns while disclosing information. Opting out is not considered an option because exclusion from the group is undesirable.

Looking at the interpersonal level, some forms of social collectives are determined by internalized emotional ties and implicit rules (Gemeinschaft/Community), whereas other collectives are determined by rational calculations and explicit rules (Gesellschaft/Society) (*Theory of Gemeinschaft and Gesellschaft*; Tönnies, 2012). In social networks, people share private information because doing so is an implicit rule for belonging to a certain group. Although people are abstractly aware of data violation, these rational feelings cannot be translated into actual feelings of fear (Gesellschaft/Society). As a result, the desire of belonging to a social network overrides any fears the consequences of data misuse might provoke (Lutz and Strathoff, 2011). Furthermore, 'impression management' in social networks plays an important role. The *Extended Two-Component Model of Self-Presentation Online* (based on Leary and Kowalski, 1990) states that self-presentation is the process by which individuals try to control the impression that others form of them. This process is determined by two components: (1) impression motivation (the desire to create or re-create impressions in others' minds; influenced by goal relevance, value of desired goal and discrepancy between desired and current self-image) and (2) impression construction (the process of creating this impression through change of behavior; influenced by self-concept, desired identity, role constraints, current or potential social image and target values). According to Krämer and Haferkamp (2011), the target value works differently in the online context compared to self-presentation in the offline context: either a wealth of information has to be given to broad audiences or vague information to avoid contradiction with others' values. The former conflicts with privacy concerns and can therefore be seen as an inhibitor to online self-presentation. The latter places constraints on the goal to provide a detailed true self. Therefore, decision processes depend on the strength of impression motivation and privacy concerns that can eventually lead to a certain paradoxical behavior of self-disclosure.

3.3.2. Privacy valuation failed

Public Value Theory (Meynhardt, 2009) states that any organization contributes to society's wellbeing (objective facts), provided that individuals perceive their relationship to the public as either positively or negatively (objective facts are reflected in people's perceptions and subjective evaluation). If an organization is perceived as trustworthy regarding data protection but their public value is low, this organization does not contribute to the public value, unless general data protection is valued by the public. This partly explains the privacy paradox as people do not engage in protective behavior because they fail to value data protection (Lutz and Strathoff, 2011). Relationships with others and how social roles, social support and social systems influence individuals' behaviors and the outcomes of such interactions are central to interpersonal relationships. Amongst others, to orient and master the social world, individuals form social representations and exchange such values, ideas or practices. As a result, new concepts are integrated into existing representations (making the unfamiliar familiar) by means of anchoring (the integration of new knowledge into existing representation) and objectification (making abstract concepts concrete by the creation of a new representation, e.g. the concept of privacy) (*Social Representation Perspective;* Abric, 1996; Moscovici, 1984). According to Oetzel and Gonja (2011), the contradictory behavior of privacy protection occurs because privacy, as a concept, is not yet integrated into an individual's social representation.

3.3.3. Knowledge deficiency due to incomplete information

In game theory, one party is usually less informed than the other. In other words, not all parties know each other's values and rules. Users may be unaware of the importance of the data they disclose and what the consequences are of disclosing personal information (e.g. data is stored and processed by third parties). Due to this unawareness, eventual risks cannot be properly evaluated and the state of incomplete information prevents users from acting rationally and maximizing benefits (*Theory of Incomplete Information*; Harsanyi, 1967). This implies that users are lacking in privacy protection knowledge, at both the technological and legal levels; leading to misinterpretation of the likelihood of actual privacy violations and to inaccurate predictions of future hazards (Acquisti and Grossklags, 2005). Furthermore, not only are individuals ignorant as to the value of their data, they are unaware of the automated collection pathways and therefore unable to calculate the consequences of data disclosure at all. Consequently, costs are neglected and benefits preferred (Deuker, 2010; Flender and Müller, 2012). A viable evaluation of potential privacy threats requires processing quite a lot of information, information users often do not have and information that would likely prove superfluous anyway, as the probability of a future privacy violation is difficult for most to reasonably judge (Acquisti, 2004). In their study on app purchase behaviors, Buck et al. (2014) suggest that some costumers engage in subconscious purchase processes and a search for relevant information about

issues such as data usage by third-parties does not even take place. The asymmetry of information possession and relying on mental short-cuts is strengthened even more by the operating systems in IOS (only one search result is prominently proposed to the users when searching for new apps) as a rule-of-thumb strategies play an important role in decision-making. As previously discussed in the *Dual Process Model of Cognition* (Kahneman, 2003), decision-making is based on System I that is fast and automatic but vulnerable to influences that inhibit the rational decision-making process (produces intuitive concern, for instance), and System II that is rational and responsible for reasoning (produces considered concern, for instance). Relying on System I, individuals act on their intuitive concern without assessing the risks due to an incomplete understanding of it. Thus, no considered concern takes place and individuals are vulnerable to heuristic thinking. (Phelan et al., 2016). Considering the interpersonal level of decision making while interacting with others, people share meaning and actions, and come to understand events in similar and certain ways (*Symbolic Interactionism;* Blumer, 1986). For instance, behavior on a social networking site can be described as a continuous process of information sharing and assessing reactions to this information from friends. By doing so, users become aware of the consequences of sharing information at a social privacy level but not at an institutional privacy level. Thus, users carefully monitor their self-presentation online but there is little or no interaction with the institutions that manage the information they disclose. This situation, in combination with low transparency as it pertains to data usage by provider companies, eventually leads to misinformation and misinterpretation of how third parties will utilize users' information and data disclosure despite privacy concerns (Young and Quan-Haase, 2013).

4. Discussion

The purpose of this paper was to review prior research on the phenomenon of the so-called privacy paradox. Based on several theoretical approaches to decision-making, we were able to review the emergence of the privacy paradox through different lenses, differentiating decision-making according to a rational risk-benefit-calculation, a biased risk-benefit calculation and a decision-making process that involves no or only negligible risk consideration. We analyzed how these various theoretical approaches explain the apparent problem of paradoxical behavior (claiming to have privacy concerns but disclosing private information nonetheless) when engaging in online media activities, especially those pertaining to mobile computing (an important contributing segment when obtaining a more complete picture of the emergence of this phenomenon). In this final section, the main conclusions from the papers analyzed are drawn and implications for design and future research directions will be given.

4.1. Categories of decision making in the context of information privacy

The systematic literature brought three decision-making categories effecting information privacy to light. First, decision-making can be divided into either a rational calculation of risk and benefits, or an irrational risk-benefit calculation characterized by biased risk assessment. Looking at the rational processes, individuals weigh costs against benefits, favoring gains over risks in most cases, such as using the service of an app or staying in contact via social network sites. Thus, information is given away in exchange for certain gratifications. Although users are aware there may be associated risks, compelling benefits or offers dull the perceived threats to privacy and safeguards are neglected. Looking at the irrational processes in decision-making, biases influencing the risk-benefit calculation play a role. Due to aspects such as heuristic thinking, (immediate) gratifications or time inconsistency, individuals are biased in their risk assessment, resulting in a distorted risk-benefit calculation, quite often tuned out to the advantages of associated benefits. The third category of decision-making describes processes in which negligible or no risk assessment takes place. Failed privacy valuations or information deficits for example, result in the risks associated with information disclosure being suppressed or even neglected altogether. All three categories of decision-making as it pertains to issues of information privacy might explain the discrepancy between stated attitudes and actual behavior, a phenomenon also known as the privacy paradox.

*4.2. Rationality versus **i**rrationality in **d**ecision-making*

We believe, that to a greater extent, decision-making takes place on an irrational level rather than on a rational one, especially when it comes to mobile computing; suggesting that decisions are highly dependent on the context in which technology is used. The environment in which mobile applications are obtained and used means the decision-making process takes place much faster and on-the-go. This is partly supported by the studies which discuss the privacy paradox with regard to mobile applications (Buck et al., 2014; Deuker, 2010; Kehr et al., 2015; Zafeiropoulou et al., 2013; Zhang et al., 2014) but challenging the assumption of a more rational view on the emergence of the privacy paradox (Park et al., 2015; Pentina et al., 2016; Poikela et al., 2015; Quinn, 2016). However, we are in favor for a mixed approach when looking for potential solutions to overcome the privacy paradox as proposed by Phelan et al. (2016) and Lutz and Strathoff (2011). According to Phelan et al. (2016) design solutions should be adapted to different cognitive styles. The actual form such solutions might take remains ambiguous. To a large extent, it seems that individuals act on their intuition without assessing potential risks with regard to privacy and security intrusion, or they have considered concern but are constrained in their actions by external factors such as low transparency, user unfriendly design or consumer hostile privacy policies with all-or-nothing usage

permissions. Sharing information (and using mobile applications) becomes a normal part of social life (Zafeiropoulou et al., 2013) and people are urged to accept certain requirements. The goal is to implement rational as well as irrational processes into design (backend and interface) so that decision-making eventually becomes self-determined. Only if this is fulfilled can a user's security and privacy concerns be diminished. Consequently, we propose to raise knowledge and awareness by design, trigger heuristics through system and interface design (Gambino et al., 2016), support users through semi-automated or predominantly automated user-centered systems and user-friendly interface designs. Furthermore, we propose to make use of interactive software and social interaction to support the user as interactive software is typically perceived to be as trustworthy as a human communication partner (Berendt et al., 2005). Learning at the moment of experience (Jia et al., 2015) and empowerment of users in their self-determined decision-making should be a top priority.

4.3. Emergence of the privacy paradox is context-dependent

This review shows that during the last three years in particular, the issue of the privacy paradox and its emergence has moved into the focus of researchers, especially in conjunction with mobile application usage. However, the majority of papers still focus on social networks and other online media. Comparing the results from social network studies with those focusing on mobile application usage, it seems that the privacy paradox within the mobile context is even more complex. This is possibly attributable to the routine, enhanced privacy policies, better technical support and comparatively long availability of online services such as social networks and e-commerce platforms, raising the question as to whether or not the same can be said of mobile applications. Restricting one's profile on social networks is the easiest way to protect against privacy threats and security intrusions. However, such protection measures are not easily accessible while downloading and installing apps, suggesting that the majority of users do not possess the expertise nor the experience to engage in what would be considered appropriate protective behavior. We would argue that the technical processes underlying mobile computing exceed the comprehension of most users. For this reason, the following question can be posed: Is the same generic term, 'privacy paradox' applicable to both stationary online activities and those considered mobile? A differentiation could open the door to a whole new area of interesting research possibilities.

4.4. Solutions to the paradoxical behavior of users

Concrete proposals designed to tackle the problem of paradoxical behavior – claiming to have privacy concerns but acting to the contrary – remain scarce. Current efforts are mainly focused on redefining guidelines for the process(s) that take place during the decision-making phase, such as the simplified possibility of restricting data access permissions during the installation of mobile applications. There are currently no viable solutions designed to span the gap between a user's intention and behavior. We believe that research into finding a solution to this problem deserves more attention. A movement to user-orientated design is needed in order to empower the user with the ability to make self-determined decisions on matters of privacy protection and online security. Shifting the reference point from 'not mine' to 'mine' goes along with higher risk perception which leads to the development of psychological ownership. This might elicit a higher valuation of private information, resulting in risk-averse decision-making (Kehr et al., 2014). Hence, individuals may be less vulnerable to disclosure influences due to their loss aversion and their sensitivity to loss (Baek, 2014). In the context of context-aware mobile applications, Deuker (2010) propose privacy disclaimers at a situation-specific level to mitigate the effects of bounded rationality. Privacy awareness tools should empower users to make well-informed decisions with regard to their information disclosure (Pötzsch et al., 2010). Furthermore, interface design should bring attention to such intentions in terms of mobilization (activating heuristics which protect the user) (Kehr et al., 2014; Kehr et al., 2015). In their study on mobile websites, Zhang et al. (2014) concluded that a security warning with regard to the website resulted in increased threat perception as it pertains to private information, negative attitudes towards the service provider and lower tendency for future use. This puts an emphasis on positive user experience to promote privacy protection behavior (Kehr et al., 2014). In the case of privacy threats, psychological reactance behavior might be triggered (Brehm, 1966) as the individual tries to reach a certain state of restored autonomy through aversive reaction in a situation in which personal freedom is threatened (e.g. limiting or denying free choice by others). In other words, as a consequence of perceived privacy threats, users might try to regain control (freedom) by providing less personal data or even avoiding situations that could place them at potential risk (e.g. a cessation of app downloading). Creating privacy awareness in combination with tools that support users in their privacy decisions should help users to avoid paradoxical behavior (Deuker, 2010).

4.5. The special case of mobile computing

The use of mobile devices and the use of mobile applications in particular, falls within the realm of personal space extension: "...smartphones felt like intimate zones and extensions of their bodies" (p. 2347; Shklovski et al., 2014). This could explain why the majority of papers discuss the privacy paradox in mobile computing through theories at the intrapersonal level where cognitive, internal processes are used to process stimuli in order to behave a certain way. It seems that the downloading and use of mobile applications is - to a greater extent - self-referential in the sense that a user's decision on whether or not to download a mobile application is done so in accordance with their personal preferences rather than those of their social group (with the exception of 'WhatsApp and other social networking apps not considered). This observation

has not been researched to date, despite the fact that this might play an inherent role in solving the privacy paradox problem. Furthermore, individuals tend to organize their use of mobile applications according to goal orientation, with users showing a higher susceptibility to accepting privacy and security intrusions (e.g. a banking app) when compared to less important applications (e.g. a gaming app) (Shklovski et al., 2014). However, research on this tendency is still scarce and should not be neglected when looking for solutions. Furthermore, app stores for the Android operating system in particular, currently employ an all-or-nothing-policy, meaning that users have to accept all permissions in order to download a particular app; suggesting a deliberate, systematic provocation of paradoxical behavior that could ultimately lead to overall acceptance of privacy risks as the stress that comes with a user's sense of inability and vulnerability dulls through continuous privacy invasion. Users express a desire for transparency and information control but are not able to act according to their needs for privacy (Shklovski et al., 2014). This makes it even harder to overcome the privacy paradox as the desire to own a particular app seems to outweigh potential risks all too often. This raises the question: To what extent is it possible to address this problem with the implementation of measures such as design prompts?

4.6. Research limitations

This review showed further limitations of the research to date. Attitude and intention are not actual behavior and actual behavior is seldom measured in the studies. Privacy concerns seem to be highly situation-dependent and can be described as a fluent concept that changes over time. However, most studies have researched privacy as a stable concept (Xu et al., 2010) or used conventional polls that are not suitable for studying online privacy (Baek, 2014). Dienlin and Trepte (2015) also rendered critique on prior measurements of the privacy paradox. When distinguishing between (i) information, (ii) social and (iii) psychological privacy, results showed that the differentiation between these privacy dimension had a direct effect on the corresponding behavior (i: preference for disguising identity = less likely identifiable on a social networking site; ii: preference for restriction profile = more restriction applied; iii: preference for less personal information = less personalized profile). Accordingly, when distinguishing between privacy concerns and attitudes, applying the appropriate theory to the problem in question (here *TPB*) and differentiating on the above mentioned privacy dimension, the authors consider the privacy paradox as 'a relic of the past' (p. 295; Dienlin and Trepte, 2015). However, we do not consider the privacy paradox as a relic of the past but we do believe that future research on the privacy paradox should try to measure actual behavior in order to get better insights into the problem.

5. Conclusion

The purpose of this article was to review prior research on the phenomenon of the privacy paradox. We highly question whether or not rational decision-making processes are the only suitable explanation for the discrepancies between privacy concerns, especially as it applies to mobile computing as decision-making in a mobile environment is subject to environmental and circumstantial factors different from those encountered during desktop computing. When analyzing the design of mobile applications, we favor a mixed approach (rational and irrational decision-making) and design solutions should be adapted to different cognitive styles. Implementing cues into the design (backend and interface) is a necessary requirement for the empowerment of the user if data protection is to become more rational. However, attempts to theoretically explain and practically solve the problem of the privacy paradox are still scarce and we feel the subject deserves far more research attention.

Acknowledgement

This work was supported by NWO, the national research council of the Netherlands (Grant number: 628.001.011) in collaboration with TNO (Dutch research institute), WODC (Dutch Research and Documentation Centre) and Centric (Dutch ICT organization).

Appendix 1. Definition of theories (in alphabetical order)

Theory	Definition
Adaptive Cognition Theory of Social Network Participation (Hu and Ma, 2010)	Users' participation in SNs consists of three phases: initial use, exploratory use and managed use. The progression from one phase to the next results from the understanding of benefits and risks and the adaptation of activities and controls. The final phase is relatively stable but can easily be damaged or altered by negative experiences or positive reinforcements. Based on rational choice theory and behaviourism.
Cognitive Heuristics (Tversky and Kahneman, 1975)	Rule-of-thumb strategies play an important role in decision

Appendix 1 (*continued*)

Theory	Definition
	making. These mental short-cuts allow individuals to come to a decision quickly without the urge to think about the next action. But heuristics can lead to biases as something that has been applicable in the past, is not necessarily suitable in another situation. Furthermore, heuristic hinders individuals from developing new ideas and alternative solutions.
Communication Privacy Management Theory (Petronio, 1991, 2002)	The decision on which information to reveal and which to keep private. Publication or retention goes along with certain risk and benefits. This process is guided by the subjective privacy boundaries individuals have (determined by an iterative process of rule development, boundary coordination, boundary turbulence) and reshaped continuously, depending on situation, context and communication partner(s).
Conformity and Peer Group Pressure (Crutchfield, 1955)	Individuals feel indirect pressure to change their own behavior in order to conform to an admired peer group. Peer group pressure can either result in positive or negative reactions (e.g. start smoking or studying regularly).
Cues-filtered-out Theory (Sproull and Kiesler, 1986, 1991)	This theory implies that individuals disclose more personal data in computer-mediated communication settings compared to face-to-face settings due to the absence of social and contextual cues.
Duality of Gemeinschaft und Gesellschaft (Tönnies, 2012)	Some forms of social collectives are determined by internalized emotional ties and implicit rules (Gemeinschaft), whereas other collectives are determined by rational calculations and explicit rules (Gesellschaft). In social networks, people share private information because this is an implicit rule for belonging to a certain group. Although people know about data violation (explicitly) albeit on an very abstract level, these rational feelings cannot be translated into actual feelings of fear (Gesellschaft). As a result, the feeling of belonging to a social network overpowers the threats of data misuse.
Dual Process Model of Cognition (Kahneman, 2003)	Decision-making is based on two systems. System I is fast and automatic but is vulnerable to influences that inhibit the rational decision-making process (produces intuitive concern for instance), whereas System II is rational and responsible for reasoning (produces considered concern, for instance). According to this theory, there are two explanations for the privacy paradox: Either individuals act on their intuitive concern without assessing the risks due to incomplete understanding of it (no considered concern takes place) or high considered concern may be overridden by low considered concern (privacy concerns are considered but individuals are unable to address them adequately).
Expectancy Theory (Vroom, 1964)	Behavior is a result of conscious choices with the purpose to maximize gain and minimize loss. This decision-making process is based on three beliefs: valence (emotional attitude towards outcome and strength of wanting a reward), expectancy (self-confidence to do s.th.) and instrumentality (perception of probability for gaining reward). Based on these beliefs, an individual chooses a certain behavior over others because of the expected outcome of that specific behavior.
Extended Two-Component Model of Self-Presentation Online (based on Leary and Kowalski, 1990)	Self-presentation (impression management) is the process by which individuals try to control the impression the make on others. This process is determined by two components: impression motivation (the willingness to create or re-create

(*continued on next page*)

Appendix 1 (*continued*)

Theory	Definition
	impressions in another's mind; influenced goal relevance, value of desired goal and discrepancy between desired and current self-image) and impression construction: the process of creating this impression through change of behavior; influenced by self-concept, desired identity, role constraints, current or potential social image and target values.
Extension to the Privacy Calculus Theory (Culnan and Armstrong, 1999)	The privacy paradox may result from misleading situational cues which bias the cognitive valuation processes (e.g. affective thinking) and the prevalence of situation-specific considerations as compared to generic attitudes. Eventually, privacy disclosure intention is determined by situational cues even if dispositional attitudes regarding privacy behavior are different to intention. The study of Kehr et al. (2015) showed that privacy decisions are driven by situation-specific privacy assessment, general dispositions (i.e. general privacy concerns, institutional trust) and affect-based heuristics (quite often subconscious processes).
Feelings-as-Information Theory (Schwarz, 2011)	Individuals rely on their feelings (mood, meta-cognition, emotion and body sensation) in decision-making processes, often leading to accurate responses but sometimes not. While in a good mood for example, people evaluate targets or situations as more positively. Furthermore, judgments are based on feelings of ease or difficulty as situations or targets which are easy to process are evaluated more positively, less risky and more valuable.
Hyperbolic Discounting Theory (Laibson, 1997)	If there is a choice, individuals usually choose a small benefit in the short term over a larger benefit in the longer term. If all choices are available on the long term, larger benefits will be chosen, even if these will occur later than smaller benefits.
Immediate Gratifications (O'Donoghue and Rabin, 2001)	Quite often, individuals encounter self-control problems due to immediate gratifications (present bias) which leads to behavior that may backfire in the long run.
Optimistic Bias Theory (Irwin, 1953)	Individuals have a tendency to underestimate the likelihood of experiencing adverse events. This might result in denying precautions which might lower risk perception.
Privacy Calculus Theory (Culnan and Armstrong, 1999)	The intention to disclose personal information is based on a rational risk-benefit calculation as perceived benefits are weighed against risk probability. If perceived benefits outweigh risks, information might be disclosed in exchange for social or economic benefit.
Privacy Regulation Theory (Altman, 1975)	Privacy is a dynamic process of interaction regulation with others. Based on internal states and external conditions, individuals determine the degree of openness. Privacy regulation should be done at an optimal level (desired level of privacy is equal to actual level). Here, trust plays an important role in the interaction regulation process which is defined by self-boundary (around a person) which is modified by self-disclosure and a dyadic boundary (ensures discloser's safety in case of violation).
Prospect Theory (Kahneman and Tversky, 1979)	Individuals do not process information in a rational way. Decision-making processes take place in two stages. During the editing stage, expected outcomes are ordered based on heuristics by setting a reference point. During the evaluation stage, outcomes lesser than the reference point are considered as losses and greater outcomes as gains. Furthermore, losses are more heavily weighted than an equal amount of gains.

Appendix 1 (*continued*)

Theory	Definition
Public Value Theory (Meynhardt, 2009)	In Public Value Theory, any organization contributes to a society's wellbeing (objective facts) as long as such individuals perceive their relationship to the public either positively or negatively (objective facts are reflected in people's perceptions and subjective evaluation). If an organization is perceived as trustworthy regarding data protection but their public value is low, this organization does not contribute to the public value, unless data protection is valued by the public. This explains partly the privacy paradox as people do not engage in protective behavior because they fail to value data protection adequately.
Quantum Theory (Based on Busemeyer et al., 2006)	Objective reality does not exist. An object can take up any possible states simultaneously as long as an individual does not evaluate it. The evaluation changes the object's state.
Rational Choice Theory of Human Behavior (Simon, 1955)	Decisions are always reasonable and logical in order to gain the greatest benefit or satisfaction in an individual's self-interest.
Rational Ignorance Theory (Downs, 1957)	The conscious choice of an individual to not pay attention to certain information is based on a cost-benefit calculation (costs of learning are disproportionate to potential benefits).
Resource Exchange Theory (Donnenwerth and Foa, 1974; Foa, 1971)	Individuals try to rationally exchange resources with others due to their wishes and needs. Furthermore, through participation in a social system, individuals may contribute to a certain group and get benefits from each other. In exchange for other resources such as money, services, time, status and love (e.g. online relationships), people are willing to provide personal resources (e.g. personal information).
Self-Control Bias (Loewenstein, 1999)	The tendency to favor immediate rewards on the short term at the expense of future risks due to lack of self-discipline.
Symbolic Interactionism (Blumer, 1986)	Social interaction creates and maintains social structures and meanings. By interacting with others over time, people share meaning and actions and come to understand events in certain and similar ways. This is the basis for society.
Social Representation Perspective (Abric, 1996; Moscovici, 1984)	Social representations are values, ideas or practices that enable individuals to orient and master the social world. By means of social exchange, new concepts are integrated into existing representations (making the unfamiliar familiar) by means of anchoring (the fit of new knowledge into existing representation is proven through anchoring) and objectification (make abstract concepts concrete via the creation of a new representation, e.g. the concept of privacy).
Structuration Theory (Giddens, 1984)	Social life is more than individual acts, yet it is determined by social forces such as traditions, institutions or moral codes. Social structures determine human behavior but can also be altered due to perception differences, ignorance or replacement. Therefore, behavior is a balance between social structures and agency, known as the ability to act on one's own free will. The structure is achieved through a dynamic process**:** Structure forms the basis for decision-making but is at the same time the outcome of it.
Theory of Bounded Rationality (Simon, 1982)	Quite often, individuals are satisfied with a solution that is good enough but not optimal due to cognitive limitations as they are unable to access and process all of the information that would be needed to do so. Even with all of the information at hand, cognitive processing would be impossible. Individuals constantly try to rationally maximize

(*continued on next page*)

Appendix 1 (*continued*)

Theory	Definition
	benefits but decision-making can only be rational within the limits of cognitive ability and available time.
Theory of Cognitive Absorption (Agarwal et al., 1997)	Individuals in the flow state, called cognitive absorption, suppress processes that call someone's attention to feelings of cognitive dissonance, leading to inappropriate privacy calculation.
Theory of Incomplete Information (Harsanyi, 1967)	In game theory, one party is less informed than the other or in other words, not all parties know each other's utilities and rules.
Theory of Reasoned Action (TRA) (Ajzen and Fishbein, 1980)/Theory of Planned Behavior (TPB) (Ajzen, 1985)	According to TRA, an individual's behavioral intention depends on their attitude towards a certain behavior and the subjective norms. The stronger the intention, the more likely that a person will engage in a certain behavior. The TPB also predicts the likelihood of an individual's intention to engage in a certain self-controlled behavior. Behavioral intention is influenced by existing attitudes as they pertain to desired outcomes, social norms and the evaluation of the risk-to-benefit ratio of that outcome (perceived behavioral control). The stronger the attitudes, perceived control and compliance with social norms, the more likely it is that individuals will engage in certain behaviors.
Theory of Ritualized Media Use (Rubin, 1984)	The use of media extends beyond satisfying information and entertainment needs to be seen as a habitual pastime that is integrated into everyday life routines that are connected to temporary structures (favorite show at a particular time) and social rituals (meeting friends to watch a show).
Theory of Under Insurance (Kunreuther, 1984)	The tendency towards reluctance to engage in privacy protection behavior against low probability but high impact/consequences events due to biased perception (event is less threatening than it actually is), underestimation of probability (as a consequence of little or no experience with the threat in question), unawareness of the threat or costs for engagement are considered as too high.
Third-Person Effect Theory (Davison, 1983)	Individuals tend to overestimate the effect of media on others while underestimating the influence on themselves (due to social desirability = denying influence goes along with self-esteem, creating social distance to a certain group and influence is self-chosen by others). As a result, individuals usually do not demonstrate the intended behavior as a response to the message.
Uses and Gratification Theory (Blumler and Katz, 1974; Katz et al., 1974)	Media use is actively determined in order to achieve and satisfy certain goals and needs among the dimension of diversion and entertainment, building and maintaining relationships and identity construction. This assumes that individuals know their needs and how to gratify them. Individuals consume certain media either for process gratification or content gratification.

References

Abric, J.C., 1996. Specific processes of social representations. Pap. Social Representations 5 (1), 77–80.

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In: EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce, USA, 21-29.

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

Agarwal, R., Sambamurthy, V., Stair, R., 1997. Cognitive absorption and the adoption of new information technologies. In: Dosier, L., Keys, J. (Eds.), Academy of Management Best Paper Proceedings. Office of Publications and Faculty Research Services in the College of Business Administration, Georgia Southern University, Statesboro, pp. 293–297.

Agarwal, R., Karahanna, E., 2000. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS Quarterly 24 (4), 665–694.
Ajzen, I., 1985. From intentions to actions: a theory of planned behavior. In: Kuhl, J., Beckman, J. (Eds.), Action-Control: From Cognition to Behavior. Springer, Heidelberg, pp. 11–39.
Ajzen, I., Fishbein, M., 1980. Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, NJ.
Alashoor, T., Baskerville, R., 2015. The privacy paradox: The role of cognitive absorption in the social networking activity. In: Thirty Sixth International Conference on Information Systems, Fort Worth, Texas, USA, 1–20.
Altman, I., 1975. The Environment and Social Behavior. Brooks/Cole, Monterey, CA.
Baek, Y.M., 2014. Solving the privacy paradox: A counter-argument experimental approach. Comput. Hum. Behav. 38, 33–42.
Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. First Monday, 11(9). Retrieved from http://firstmonday.org/article/view/1394/1312.
Berendt, B., Günther, O., Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. Commun. ACM 48 (4), 101–106.
Blumer, H., 1986. Symbolic Interactionism: Perspectives and Method. University of California Press, Berkeley.
Blumler, J.G., Katz, E., 1974. The Uses of Mass Communications: Current Perspectives on Gratifications Research. Sage Beverly Hills, CA.
Brehm, J.W., 1966. A Theory of Psychological Reactance. Academic Press, London.
Buck, C., Horbel, C., Germelmann, C.C., Eymann, T., 2014. The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers. In: Twenty Second European Conference on Information Systems, Tel Aviv, Israel, 1–14.
Busemeyer, J., Wang, Z., Townsend, J., 2006. Quantum dynamics of human decision making. J. Math. Psychol. 50, 220–241.
Chen, H.-T., Chen, W., 2015. Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychol. Behav. Social Networking 18 (1), 13–19.
Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organ. Sci. 10 (1), 340–347.
Crutchfield, R.S., 1955. Conformity and character. Am. Psychol. 10 (5), 191–198.
Davison, W., 1983. The third-person effect in communication. Public Opin. Q. 47 (1), 1–15.
Debatin, B., Lovejoy, J.P., Horn, A.-K., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput.-Mediated Commun. 15, 83–108.
Deuker, A., 2010. Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. In: Bezzi, M., Duquenoy, P., Fischer-Hüber, S., Hansen, M., Zhang, G. (Eds.), Privacy and Identity Management for Life. Springer-Verlag, Berlin, Heidelberg, pp. 275–283.
Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.
Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Inf. Syst. J. 17 (1), 61–80.
Donnenwerth, G.V., Foa, U.G., 1974. Effect of resource class on retaliation to injustice in interpersonal exchange. J. Pers. Soc. Psychol. 29 (6), 785–793.
Downs, A., 1957. An economic theory of political action in a democracy. J. Political Economy 65 (2), 135–150.
Flender, C., Müller, G., 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Busemeyer, J., Dubois, F., Lambert-Mogiliansky, A., Melucci, M. (Eds.), Quantum interaction. Lecture notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, pp. 148–159. 7620.
Foa, U.G., 1971. Interpersonal and economic resources. Science 171 (3969), 345–351.
Gambino, A., Kim., J., Sundar, S.S., Ge, J., Rosson, M.B., 2016. User disbelief in privacy paradox: Heuristics that determine disclosure. CHI 2016. San Jose, CA, USA, 2837-2842.
Giddens, A., 1984. The Constitution of Society: Outline of the Theory of Structuration. University of California Press, Oakland.
Harsanyi, J.C., 1967. Games with incomplete information played by "Bayesian" players, I-III Part I. The basic model. Manage. Sci. 14 (3), 159–182.
Hu, Q., Ma, S., 2010. Does privacy still matter in the era of Web 2.0? A qualitative study of user behavior towards online social networking activities. In: Proceedings of Pacific Asia Conference on Information Systems (PACIS 2010), Taipei, Taiwan, 2, pp. 591–602.
Hughes-Roberts, T., 2012. A cross-disciplined approach to exploring the privacy paradox: explaining disclosure behaviour using the theory of planned behavior. In: UK Academy for Information Systems Conference Proceedings, Paper 7.
Hughes-Roberts, T., 2013. Privacy and social networks: Is concern a valid indicator of intention and behaviour?. In: International Conference on Social Computing, Washington, D.C., USA, 909–912.
Irwin, F.W., 1953. Stated expectations as functions of probability and desirability of outcomes. J. Pers. 21 (3), 329–335.
Jia, H., Wisniewski, P., Xu, H., Rosson, M.B., Carroll, J.M., 2015. Risk-taking as a learning process for shaping teen's online information privacy behaviors. In: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, Vancouver, BC, Canada, 583-599.
Joinson, A.N., Reips, U.-D., Buchanan, T., Paine Schofield, C.B., 2010. Privacy, trust, and self-disclosure online. Hum.-Comput. Interact. 25, 1–24.
Kahneman, D., 2003. Maps of bounded rationality: Psychology for behavioral economics. Am. Econ. Rev. 93 (5), 1449–1475.
Kahneman, D., Tversky, A., 1979. Prospect theory: an analysis of decision under risk. Econometrica 47 (2), 263–291.
Katz, E., Blumler, J.G., Gurevitch, M., 1974. Uses and gratifications research. Public Opin. Q. 37 (4), 509–523.
Kehr, F., Wentzel, D., Kowatsch, T., 2014. Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure. In: Thirty Fifth International Conference on Information Systems, Auckland, New Zealand, 1–12.
Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25 (6), 607–635.
Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: R-examining privacy calculus with actual user behavior. Int. J. Hum Comput Stud. 71, 1163–1173.
Kelley, P.G., Cranor, L.F., Sadeh, N., 2013. Privacy as part of the app decision-making process. CHI 2013, 1–11.
Kim, G.S., Park, S.-B., Oh, J., 2008. An examination of factors influencing consumer adoption of short message service (SMS). Psychol. Market. 25 (8), 769–786.
Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134.
Krämer, N.C., Haferkamp, N., 2011. Online self-presentation: balancing privacy concerns and impression construction on social networking sites. In: Trepte, S., Reinecke, L. (Eds.), Privacy Online. Springer-Verlag, Berlin, Heidelberg, pp. 127–141.
Kunreuther, H., 1984. Causes of underinsurance against natural disasters. Geneva Pap. Risk Insurance 9, 206–220.
Laibson, D., 1997. Golden eggs and hyperbolic discounting. Quart. J. Econ. 62 (2), 443–477.
Leary, M.R., Kowalski, R.M., 1990. Impression management: a literature review and two-component model. Psychol. Bull. 107, 34–47.
Loewenstein, G., 1999. Because it is there: The challenge of mountaineeringEllipsisfor utility theory. Kyklos 52 (3), 315–344.
Li, Y., 2012. Theories in online information privacy research: a critical review and an integrated framework. Decis. Support Syst. 54, 471–481.
Li, H., Sarathy, R., Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. J. Comput. Inf. Syst. 51 (1), 62–71.
Lutz, C., Strathoff, P., 2011. Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In: Brändli, S., Schister, R., Tamò, A. (Eds.), Multinationale Unternehmen Und Institutionen Im Wandel – Herausforderungen Für Wirtschaft, Recht Und Gesellschaft. Stämpfli Verlag, Bern, pp. 81–99.
Manier, M.J., O'Brien Louch, M., 2010. Online social networks and the privacy paradox: a research framework. Issues Inf. Syst. XI (1), 513–517.
Meynhardt, T., 2009. Public value inside: what is public value creation? Int. J. Public Administration 32 (3–4), 192–219.
Moscovici, S., 1984. The phenomenon of social representations. In: Farr, R.M., Moscovici, S. (Eds.), Social Representations. University Press, Cambridge, pp. 3–69.

Motiwalla, L.F., Li, X., Liu, X., 2014. Privacy paradox: Does stated privacy concerns translate into the valuation of personal information?. In: Proceeding of the 19th Pacific Asia Conference on Information Systems (PACIS 2014), Paper 281.
Nagy, J., Pecho, P., 2009. Social networks security. In: Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, Athens/Glyfada, Greece, pp. 740–746.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Affairs 41 (1), 100–126.
Novak, T.P., Hoffman, D.L., 2008. The fit of thinking style and situation: new measures of situation-specific experiential and rational cognition. J. Consum. Res. 36 (6), 56–72.
O'Donoghue, T., Rabin, M., 2001. Choice and procrastination. Quart. J. Econ. 116 (1), 121–160.
Oetzel, M.C., Gonja, T., 2011. The online privacy paradox: A social representations perspective. In: Paper presented at the Proceedings of the 2011 Annual Conference Extended Abstracts on Human factors in Computing Systems, Vancouver, BC, Canada.
Oomen, I., Leenes, I., 2008. Privacy risk perceptions and privacy protection strategies. In: de Leeuw, E., Fischer-Hübner, S., Tseng, J., Borking, J. (Eds.), Policies and Research in Identity Management. Springer Verlag, Boston, pp. 121–138.
Park, Y., Ju, J., Ahn, J-H., 2015. Are people really concerned about their privacy?: Privacy paradox in mobile environment. In: The Fifteenth International Conference on Electronic Business, Hong Kong, 123–128.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comput. Hum. Behav. 65, 409–419.
Petronio, S., 1991. Communication boundary management: a theoretical model of managing disclosure of private information between married couples. Commun. Theory 1 (4), 311–335.
Petronio, S., 2002. Boundaries of Privacy: Dialectics of Disclosure. State University of New York Press, Albany, NY.
Phelan, C., Lampe, C., Resnick, P., 2016. It's creepy, but it doesn't bother me. CHI 2016, San Jose, CA, USA, 5240-5251.
Poikela, M., Schmidt, R., Wechsung, I., Mueller, S., 2015. FlashPolling privacy: The discrepancy of intention and action in location-based poll participation. In: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka, Japan, 813–818.
Pötzsch, S., 2009. Privacy awareness: a means to solve the privacy paradox? In: Vashek, M., Fischer-Hübner, S., Cvrček, D., Švenda, P. (Eds.), The Future of Identity in the Information Society. Springer-Verlag, Berlin Heidelberg, pp. 226–236.
Pötzsch, S., Wolkerstorfer, P., Graf, C., 2010. Privacy-awareness information for web forums: Results from an empirical study. In: Proceedings: NordiCHI 2010, Reykjavik, Iceland, 363–372.
Quinn, K., 2016. Why we share: a uses and gratifications approach to privacy regulation in social media use. J. Broadcast. Electron. Media 60 (1), 61–86.
Rubin, A.M., 1984. Ritualized and instrumental television viewing. J. Commun. 34, 67–77.
Schwarz, N., 2011. Feelings-as-information theory. In: Van Lange, P., Kruglanski, A., Higgins, E.T. (Eds.), Handbook of Theories of Social Psychology. SAGE Publications Ltd, UK, London, pp. 289–308.
Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H., 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. CHI 2014, Toronto, ON, Canada, 2347-2356.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Quarterly 35 (4), 989–1015.
Smith, E.J., Kollars, N.A., 2015. QR panopticism: user behavior triangulation and barcode-scanning applications. Inf. Secur. J. Global Perspect. 24 (4–6), 157–163.
Simon, H.A., 1955. A behavioural model of rational choice. Q. J. Econ. 69 (1), 99–118.
Simon, H.A., 1982. Models of Bounded Rationality. MIT Press, Cambridge, MA.
Sproull, L., Kiesler, S., 1986. Reducing social context cues: electronic mail in organizational communication. Manage. Sci. 32 (11), 1492–1512.
Sproull, L., Kiesler, S., 1991. Connections: New Ways of Working in the Networked Organization. MIT Press, Cambridge, MA.
Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. In: Proceedings of CHI'13 Extended Abstracts on Human Factors in Computing Systems, France, 811–816.
Tönnies, F., 2012. Studien Zu Gemeinschaft Und Gesellschaft. Springer, Wiesbaden.
Tsai, J., Cranor, L., Acquisti, A., Fong, C., 2006. What's it for you? A survey of online privacy concerns and risk. NET Institute Working Paper, No. 06–29, 1–20.
Tversky, A., Kahneman, D., 1975. Judgment under uncertainty: Heuristics and biases. Utility, Probability, and Human Decision Making. Springer, The Netherlands.
Vroom, V.H., 1964. Work and Motivation. Wiley, New York.
Wakefield, R., 2013. The influence of user affect in online information disclosure. J. Strategic Inf. Syst. 22, 157–174.
Wilson, D.W., Valacich, J.S., 2012. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. In: Thirty Third International Conference on Information Systems, Orlando, Florida, 1-11
Xu, H., Teo, H.-H., Tan, B.C.Y., Agarwal, R., 2010. The role of push-pull technology in privacy calculus: the case of location-based services. J. Manage. Inf. Syst. 26 (3), 135–173.
Yoo, C.W., Ahn, H.J., Rao, H.R., 2012. An exploration of the impact of information privacy invasion. In: Proceeding of Thirty Third International Conference on Information Systems, Orlando, Florida, 1–18.
Young, A.L., Quan-Haase, A., 2013. Privacy protection strategies on Facebook. Inf. Commun. Soc. 16 (4), 479–500.
Zafeiropoulou, A.M., Millard, D.E., Webber, C., O'Hara, K., 2013. Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions?. In: WebSci '13 Proceedings of the 5th Annual ACM Web Science Conference, New York, USA, 463–472.
Zhang, B., Wu, M., Kang, H., Go, E., Sundar, S.S., 2014. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In: Toronto, O.N. (Ed.), CHI 2014. Canada, pp. 111–114.